ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ESTUDIO Y DISEÑO DE LA RED PORTADORA DE TELECOMUNICACIONES, PERTENECIENTE A LA EMPRESA ECUAONLINE S.A., QUE PERMITA BRINDAR SERVICIOS DE INTERNET UTILIZANDO IPNG (IPv6) PARA LOS USUARIOS DE LAS CIUDADES DE QUITO, CAYAMBE, LATACUNGA, OTAVALO E IBARRA

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

GABRIEL ANDRÉS BONILLA BAUS
gabo_ab100@hotmail.com

DIRECTOR: DR. LUIS ANIBAL CORRALES PAUCAR
luis.corrales@epn.edu.ec
CODIRECTOR: ING. PABLO WILLIAM HIDALGO LASCANO
pablo.hidalgo@epn.edu.ec

Quito, julio 2016

DECLARACIÓN

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

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

Gabriel Andrés Bonilla Baus

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Gabriel Andrés Bonilla Baus, bajo nuestra supervisión.

Dr. Luis Anibal Corrales Paucar DIRECTOR DEL PROYECTO	Ing. Pablo William Hidalgo Lascano CODIRECTOR DEL PROYECTO

AGRADECIMIENTO

Quiero agradecer a Dios por permitir culminar este proyecto tan importante en mi vida. A mi familia quienes con su esfuerzo y preocupación supieron encaminarme por el mejor camino del bien. A mis abuelitas quienes mostraron su preocupación constante en este camino tan largo de mi vida. A mis padres quienes con su amor y entrega me dieron la mejor educación posible. A mi novia Anita quien me entregó todo su amor, cariño y preocupación para lograr mis metas y objetivos. A mi hija Anapaula que fue quien me impulsó a culminar lo propuesto.

A todos quienes estuvieron de una u otra forma preocupados por mi bienestar.

Gracias.

Gabriel Andrés Bonilla Baus.

DEDICATORIA

Quiero dedicar el presente proyecto de investigación, primero a mis padres, ya que sin su apoyo, este objetivo no tuviera significado. Ellos han sido el principal soporte durante toda mi vida y me han sabido encaminar de la mejor manera.

En segundo lugar a mi nueva familia, mi Anita y mi hija Anapaula, ya que por ellas entregaría el mayor de mis esfuerzos. Uds. son el motor que mueve mis sentidos. Los Amo a todos.

Gabriel Andrés Bonilla Baus.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

RESUMEN

En la actualidad, Internet es una herramienta tan cotidiana que ni siquiera la población se ha dado el tiempo de pensar si estamos preparados para vivir sin ella.

La masificación de Internet en todo el mundo, el explosivo aumento de dispositivos conectados a la red y la mala política inicial de asignación de las direcciones, han acelerado en todo el mundo el agotamiento de las direcciones IP versión 4 (IPv4)

Una dirección de Protocolo de Internet (IP) identifica con números únicos a cada dispositivo conectado a Internet, que son usados para mover o direccionar toda la información que se transmite en Internet, ya sea para revisar *e-mail* o acceder a páginas *Web*. Estas direcciones son la cuarta versión del protocolo IP (IPv4) y se usan desde la década de los 80. La cantidad de números disponibles es finito y, en el caso de IPv4, fue originalmente de 4 mil millones de direcciones, es decir, 2^{32}.

Después de años de crecimiento y desarrollo de Internet, estamos acercándonos al límite máximo de direcciones IP, no porque hayamos conectado 4 mil millones de computadores sino porque existen tasas de pérdida enormes en la asignación, que partió haciéndose en forma desordenada y que recién en los últimos años se ha racionalizado, demorando esta fecha límite en que no quedarán más direcciones IPv4 que asignar.

El diseño presentado tiene como principal objetivo proveer de tráfico IPv4 e IPv6 paralelamente, con el argumento de que la transición a IPv6 nativo se realice de forma paulatina y escalonada, para que finalmente, en algunos años, se pueda ofrecer completamente o en su gran mayoría tráfico IPv6 al 100%.

El resultado de este estudio y diseño, que está enfocado en la red del proveedor Ecuaonline S.A, desemboca en una infraestructura adecuada para trabajar en Doble Pila desde el *Core* de la red, hasta el usuario final, con lo que se garantiza que el tráfico IPv4 e IPv6 puede transitar de forma paralela en la red del proveedor hacia el Internet.

Se obtiene, como parte de este estudio, un presupuesto estimado para poder cumplir el objetivo del proyecto, lo que involucra que se deban realizar ciertos cambios de hardware y software en la red del proveedor actual.

En el primer capítulo se realizó un análisis de los protocolos IPv4 e IPv6 en donde se describen las limitaciones que presenta IPv4; se estudia IPv6 describiendo las características principales y, las ventajas y desventajas entre los 2 protocolos.

El primer capítulo también está enfocado en revisar el direccionamiento del protocolo IPv6 que incluye: prefijos y tipos de direcciones IPv6, así como también el estudio de los mecanismos de transición de IPv4 a IPv6.

En el capítulo dos se revisa la estructura actual de la empresa Ecuaonline S.A. dentro de cada una de sus redes: *core*, distribución y acceso. Se concluye que hay algunos equipos que soportan IPv6 y otros que no.

En el capítulo tres se realizó el diseño de la red de portadora de Telecomunicaciones Ecuaonline S.A. con el protocolo IPv6, que incluye: rangos de direccionamiento a entregar a cada ciudad, mecanismo de transición elegido, proveedores de servicio de Internet IPv6 nativo y prefijo IPv6 requerido para cubrir las necesidades de los clientes en todas las ciudades.

Para hacer este estudio, se definieron los nuevos equipos que son necesarios instalar en la red de Ecuaonline S.A. con el fin de que los mismos permitan cursar tanto trafico IPv4 como trafico IPv6.

En el cuarto capítulo se presenta un estudio de costos que incluyó precios referenciales de equipos con soporte IPv6, costo de instalación del proveedor IPv6 y costo final del proyecto presentado.

Las conclusiones y recomendaciones obtenidas con el desarrollo del presente proyecto se presentan en el capítulo cinco.

PRESENTACIÓN

La necesidad de implementar soluciones reales para la transición al nuevo estándar IPv6 se debe principalmente a la falta de direcciones que ofrece IPv4 en la actualidad.

Por la gran demanda de direccionamiento público, que día a día requieren los usuarios para conectar distintos dispositivos al Internet, es necesario adoptar un nuevo estándar que permita interconectar millones de equipos entre sí.

Este estándar, denominado IPv6, tiene un espacio de direccionamiento de 128 bits, es decir 2^{128} equivalente a 340 sextillones direcciones públicas, (340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones posibles), lo que permitirá satisfacer las exigencias en cuanto a direccionamiento se refiere.

Frente al problema de escasez con IPv4 (únicamente 2^{32} direcciones públicas posibles) se planteó realizar un diseño y estudio de la red portadora de Telecomunicaciones Ecuaonline S.A., utilizando el nuevo protocolo IP versión 6, para dar servicio de Internet a los usuarios de Quito, Cayambe, Latacunga, Otavalo e Ibarra, con los cual, el proveedor Ecuaonline S.A. tendrá la capacidad a futuro de utilizar este diseño para implementar en su red y ofrecer nuevos servicios y oportunidades a sus clientes finales.

Este proyecto de titulación está dirigido a estudiantes de ingeniería en redes, telecomunicaciones, personas que trabajen en empresas proveedoras de Internet, administradores de red en ISPs y en general a cualquier persona que desee aplicar el nuevo protocolo IPv6 en proyectos de redes y *networking*.

CAPÍTULO 1

ESTUDIO DE LOS PROTOCOLOS IPv4 E IPv6

1.1 INTRODUCCIÓN

Es un hecho que las tecnologías de información y comunicación (TIC) se han convertido en una parte esencial en la vida cotidiana de los seres humanos. En los últimos años la evolución de esta tecnología se ha desarrollado de una manera muy acelerada y ha influido en la forma de comunicarse y relacionarse con las personas a lo largo del mundo. Poco a poco se observa cómo los medios tradicionales de comunicación (televisión, radio, telefonía, entre otros) convergen hacia una única red de comunicaciones como lo es, el Internet.

Esta forma de encaminarse hacia un solo medio ha llevado a un crecimiento significativo en el número de usuarios de Internet. Conjuntamente, Internet ha evolucionado de ser una simple red que conecta pocos computadores, a una plataforma completa que ofrece distintos tipos de servicios. Esta tendencia de evolución deja al descubierto las limitaciones que el protocolo IP versión 4 presenta.

IPv4 fue desarrollado en septiembre de 1981 [1] como una forma de interconectar un número limitado de redes, pero jamás se pensó que ésta sería la base para la comunicación entre millones de usuarios. Su pequeño número de direcciones disponibles (4.294.967.296 direcciones) junto con su problema de arquitectura han frenado el desarrollo de nuevas aplicaciones y tecnologías en Internet.

El protocolo IPv6 se desarrolló durante la década de los años 90 con el fin de reemplazar a IPv4 como protocolo dominante en Internet. El protocolo IPv6 soluciona los principales inconvenientes que IPv4 presenta y entrega un avance para futuros desarrollos y avances en Internet. Una de las principales ventajas que el protocolo IPv6 presenta es el gran número de direcciones de red disponibles para miles de millones de dispositivos y usuarios finales.

Actualmente empresas y organizaciones en muchas partes del mundo no encuentran aún motivos suficientes para invertir en implementaciones IPv6. Se estima que ese comportamiento cambie a medida que se desarrollan nuevos servicios y tecnologías que requieran un acceso masivo a Internet, tales como los ofrecidos por las tecnologías 3G & 4G.

El método actual y tradicional por medio del cual empresas, universidades y usuarios finales han realizado implementaciones de redes IPv6 es mediante el uso de mecanismos de transición basados en túneles.

1.2 PROTOCOLO DE INTERNET VERSIÓN 4 (IPv4)

En este subcapítulo se estudiará brevemente la estructura del protocolo de Internet versión 4.

1.2.1 CARACTERÍSTICAS DEL PROTOCOLO DE INTERNET VERSIÓN 4

- Protocolo de conmutación de paquetes, tanto a nivel de servicio como de implementación.
- No orientado a conexión. Cada paquete se enruta de forma independiente.
- No garantiza ni la entrega, ni el orden, ni la no duplicidad de la información.
- Es un protocolo no confiable.
- No detecta ni corrige errores en el *Payload*[1], solo detecta errores en el encabezado descartando el paquete cuando éste llega mal.
- Soporta fragmentación al pasar por redes de diferente MTU[2].
- Define claramente la unidad de transferencia denominada datagrama o paquete IP.

[1] Carga útil. Máximo 65.535 bytes
[2] MTU representa la unidad máxima de transferencia.

- Hace ver el conjunto de redes físicas como una sola red virtual (Internet).

1.2.2 ESTRUCTURA DEL PAQUETE IPv4

Los campos que componen la cabecera IPv4 se muestran en la Figura 1.1 y la descripción de cada uno de los campos se amplía de mejor manera en la Tabla 1.1.

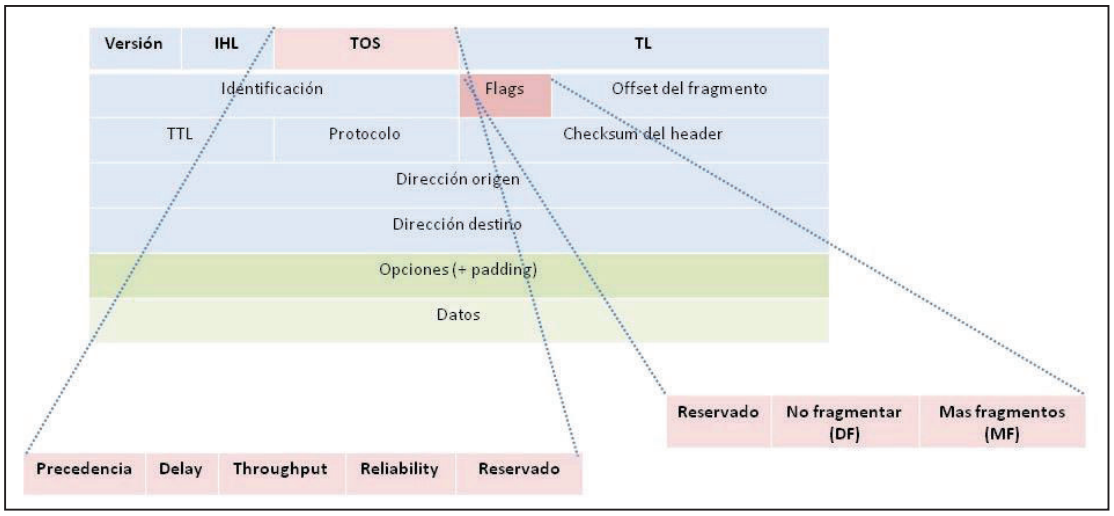


Figura 1.1 Arquitectura del paquete IPv4

Tabla 1.1 Descripción de los campos del paquete IPv4

Nombre del campo	Tamaño (bytes)	Descripción
Versión	½ (4 bits)	**Versión:** Identifica la versión de IP que se utiliza para generar el datagrama. Para IPv4, esto es, por supuesto el número 4. El propósito de este campo es garantizar la compatibilidad entre dispositivos que están ejecutando diferentes versiones de IP. En general, un dispositivo que ejecuta una versión anterior de IP rechaza los datagramas creados por nuevas implementaciones, bajo el supuesto de que la versión anterior puede no ser capaz de interpretar los nuevos datagramas
IHL	½ (4 bits)	**Internet *Header Length* (IHL):** Especifica la longitud de la cabecera IP, en palabras de 32 bits. Esto incluye la longitud de los campos "**Descripción** de opciones" y el "relleno". El valor normal de este campo cuando no se utilizan las opciones es de 5 (cinco palabras de 32 bits = 5 * 4 = 20 bytes).

Nombre del campo	Tamaño (bytes)	Descripción
TOS	1	**Tipo de servicio (TOS):** Es un campo diseñado para llevar la información y proporcionar calidad de servicio, tales como entrega con prioridad, para los datagramas IP. Nunca fue usado ampliamente como se había definido, y su significado ha sido posteriormente redefinido para el uso de una técnica llamada de servicios diferenciados (DS).
TL	2	**Longitud Total (LT):** Especifica la longitud total en bytes del datagrama IP. Dado que este campo es de 16 bits de ancho, la longitud máxima de un datagrama IP es de 65.535 bytes.
Identificación	2	**Identificación:** Este campo contiene un valor de 16 bits que es común a cada uno de los fragmentos al que pertenecen en un mensaje en particular. Este campo es utilizado por el receptor para re-ensamblar los mensajes sin mezclar accidentalmente fragmentos de mensajes diferentes. Esto es necesario porque los fragmentos pueden llegar desde múltiples mensajes mezclados entre sí, ya que los datagramas IP pueden ser recibidos desordenadamente desde cualquier dispositivo.
Banderas	3/8 (3 bits)	**Banderas:** *Se revisará en la Tabla 1.2.*
Desplazamiento del fragmento	1 5/8 (13 bits)	***Offset* del Fragmento:** Este campo especifica el desplazamiento o la posición, en el mensaje general cuando un mensaje se ha fragmentado. Se especifica en unidades de 8 bytes (64 bits). El primer fragmento tiene un desplazamiento de valor 0.
TTL	1	***Time to Live* (TTL):** Especifica el tiempo que se le permite "vivir" al datagrama en la red, en términos de saltos de enrutador. Cada enrutador disminuye el valor del campo TTL (lo reduce en 1) antes de retransmitirlo. Si el campo TTL llega a cero, el datagrama se descarta.
Protocolo	1	**Protocolo:** Identifica el protocolo de capa superior (generalmente puede ser un protocolo de capa transporte o de red) transportado en el datagrama. El valor de este campo fue definido originalmente por la norma "Asignación de números" por la IETF, RFC 1700, y ahora es mantenido por la IANA. Ver Tabla 1.3.
Suma de verificación del *Header* (*Checksum*)	2	***Checksum* de la cabecera:** La suma de comprobación del encabezado es una protección básica contra la corrupción en la transmisión. Este no es el código CRC más complejo que suelen utilizar las tecnologías de la capa de enlace de datos como *Ethernet*, es sólo una suma de comprobación de 16 bits. Se calcula dividiendo los bytes de cabecera en palabras

Nombre del campo	Tamaño (bytes)	Descripción
		(una palabra es de dos bytes) y luego sumándolos. Los datos no son comprobados, sólo el encabezado. En cada salto el dispositivo receptor del datagrama realiza la misma comprobación y si hay error, descarta el datagrama dañado.
Dirección Origen	4	**Dirección Origen:** Dirección IP de 32 bits del emisor del datagrama. Tenga en cuenta que a pesar de que los dispositivos intermedios, tales como *routers* pueden manejar el datagrama, no suelen poner su dirección en este campo- que siempre es el del dispositivo que originalmente envió el datagrama.
Dirección Destino	4	**Dirección Destino:** Dirección IP de 32 bits del destinatario del datagrama. Una vez más, a pesar de que dispositivos como *routers* pueden ser los objetivos intermedios de los datagramas, este campo es siempre para el destino final.
Opciones	Variable	**Opciones:** Uno o más de varios tipos de opciones se pueden incluir después de las cabeceras estándar en ciertos datagramas IP.
Rellenado (*Padding*)	Variable	***Padding*:** Si una o más opciones se incluyen, y el número de bits utilizados para ellas no es un múltiplo de 32, se añaden los ceros suficientes para "rellenar" el *header* a un múltiplo de 32 bits (4 bytes).
Datos	Variable	**Datos:** Los datos que se transmiten en el datagrama, ya sea un mensaje íntegro de capas superiores o el fragmento de un mensaje.

Tabla 1.2 Descripción del campo Banderas

NOMBRE DEL SUBCAMPO	TAMAÑO (Bytes)	DESCRIPCIÓN
Reservado	1/8 (1bit)	Reservado (no se usa)
DF	1/8 (1 bit)	**No Fragmentar:** Cuando está en uno especifica que el datagrama no debe ser fragmentado. Dado que el proceso de fragmentación generalmente es invisible para las capas superiores, la mayoría de los protocolos no se ocupan de esto y no setean esta bandera. Aun así se usa para comprobar la unidad de transmisión máxima (MTU) de un enlace.
MF	1/8 (1 bit)	**Más fragmentos:** Cuando está a cero, indica el último fragmento en el mensaje, cuando está a uno, indica que hay más fragmentos por venir del mensaje fragmentado. Si se setea la bandera de no fragmentar un mensaje entonces solo

NOMBRE DEL SUBCAMPO	TAMAÑO (Bytes)	DESCRIPCIÓN
		existirá un "fragmento" (todo el mensaje), y esta bandera estará en cero. Si se emplea la fragmentación todos los fragmentos excepto el último, lo pondrán a uno, de modo que el receptor sepa cuándo se han enviado todos los fragmentos.

Tabla 1.3 Campo Protocolo

VALOR (HEXADECIMAL)	VALOR (DECIMAL)	PROTOCOLO
00	0	Reservado
01	1	ICMP (*Internet Control Message Protocol*)
02	2	IGMP (*Internet Group Management Protocol*)
03	3	GGP (*Gateway To Gateway Protocol*)
04	4	Encapsulado IP-en-IP
06	6	TCP (*Transmission Control Protocol*)
08	8	EGP (*Exterior Gateway Protocol*)
11	17	UDP (*User Datagram Protocol*)
32	50	Extensión de encapsulado **ESP** (*Encapsulating Security Payload*)
33	51	Extensión de encapsulado **AH** (*Authentication header*)

1.2.3 PROBLEMAS QUE PRESENTA EL PROTOCOLO IPv4

Ya se mencionó que el protocolo de Internet (IP) es un protocolo de conmutación de paquetes no orientado a conexión, ya que cada paquete se enruta de manera independiente; además es un protocolo no confiable por no dar garantías de entrega, orden y la no duplicidad de la información, el cual se usa para transportar información a través de una red de paquetes conmutados.

IP se presenta en la capa 3 del modelo ISO/OSI [2] y su función es entregar paquetes desde un nodo de origen a uno de destino, basado en la dirección destino y dirección origen que cada paquete lleva. IPv4 es el protocolo que domina actualmente la red Internet, utilizada para conectar redes de forma interna y hacia el exterior.

La versión del protocolo de Internet usada actualmente no ha cambiado mucho desde su publicación en 1981. IPv4 ha demostrado ser un protocolo fácil de implementar y con la capacidad de operar sobre diversos protocolos de capa 2 como HDLC (*High Level Data Link Control*) [3], *Frame Relay* [4], PPP (*Point to Point Protocol*) [5], entre otros.

Inicialmente se lo diseñó para interconectar pocos computadores en redes simples pero conforme avanzaron nuevas necesidades ha sido capaz de soportar el asombroso crecimiento de Internet. Sin embargo, en los últimos tiempos se ha empezado a notar diversos problemas que presenta IPv4 asociado a la aparición de nuevas tecnologías y servicios que requieren conectividad IP.

1.2.4 AGOTAMIENTO DE DIRECCIONES IPv4

Una dirección de Internet versión 4 tiene un tamaño de 32 bits, lo que permite un máximo de 2^{32} (4.294.967.296) direcciones posibles a asignar. Al comienzo de su implementación, se utilizaron métodos de distribución poco eficientes, como la asignación por clases, mediante los cuales se asignaron grandes bloques de direcciones a organizaciones que no lo requerían. Esto ha generado que actualmente muchas organizaciones cuenten con un gran número de direcciones que no se encuentran utilizadas.

Los primeros reportes de alerta sobre el amenazador agotamiento de direcciones IPv4 se dieron a conocer alrededor de 1990. Varias soluciones y protocolos han permitido extender la vida útil de IPv4, tales como: enrutamiento sin clases entre dominios (CIDR – *Classless Inter Domain Routing*) [6], uso de asignaciones temporales de direcciones con servicios tales como DHCP, direccionamiento privado y la traducción de direcciones de red (NAT),

Toda la distribución está organizada por la IANA (*Internet Assigned Numbers Authority*), que es un departamento de ICANN (*Internet Corporation for Assigned Names and Numbers*), conjuntamente con los Registros Regionales de Internet (RIRs o *Regional Internet Registers*), que se ocupan de la asignación de estos recursos de numeración (direcciones IP).

En la actualidad, existen, RIRs, para las regiones de Europa y Oriente Medio (RIPE NCC), Norteamérica (ARIN), Asia Pacifico (APNIC), Latinoamérica y Caribe (LACNIC) y África (AfriNIC), que autogobiernan la gestión de los recursos públicos dentro de cada región por medio de políticas regionales establecidas por la propia comunidad, así como los recursos de forma global, por medio de políticas globales. La jerarquía de organizaciones se muestra en la Figura 1.2.

El IANA establece que las direcciones sean repartidas en 256 bloques de 8 bits (los 8 bits superiores de las direcciones IPv4), transfiriéndolos a cada uno de los RIRS desde el almacenamiento central en IANA, para su gestión regional, según se vayan agotando los recursos de cada una de dichas regiones. Estos bloques, siguiendo la nomenclatura técnica, se denominan prefijos /8.

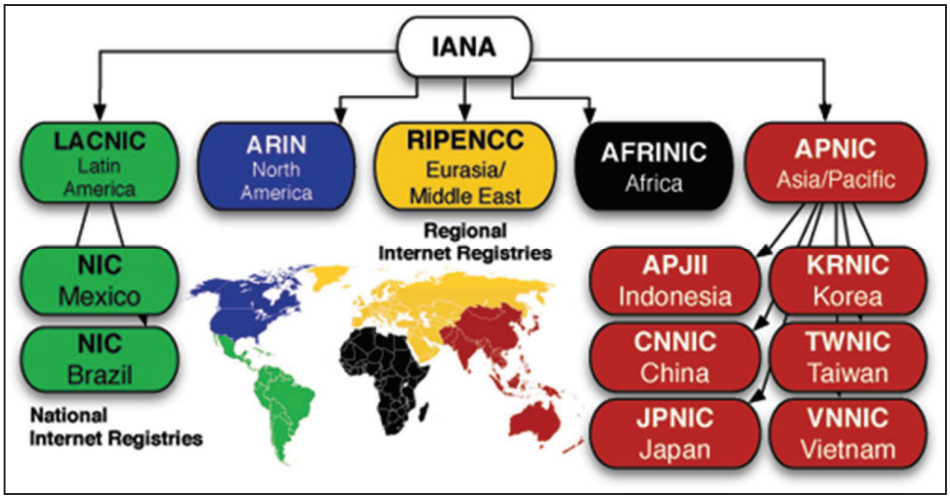


Figura 1.2 Jerarquía de organizaciones *[7]*

Los prefijos /8 utilizables en Internet son 220 ya que el rango de direcciones comprendido entre 224.XXX.XXX y 239.XXX.XXX se encuentra reservado para tráfico "*multicast*", y el rango entre 240.XXX.XXX y 254.XXX.XXX se encuentra reservado para trabajos experimentales. En la Figura 1.3 se observa la distribución actual de bloques /8.

Como se señaló en el RFC 5735 (*Special Use* IPv4 *Addresses*) una serie de bloques de direcciones son "reservados". Hay un total del equivalente de 35,3282 /8, que son "reservados por la IETF". (Esta se compone de 16 bloques /8

reservados para su uso en escenarios de *multicast*, 16 /8 bloques reservados para algún uso futuro no especificado, un /8 (0.0.0.0 /8) para la identificación local, un /8 para *loopback* (127.0.0.0 /8), y un /8 reservadas para uso privado (10.0.0.0 /8)). Pequeños bloques de direcciones también están reservados para otros usos especiales).

Los restantes 220,6718 /8 bloques de direcciones se hicieron disponibles para uso público IPv4 de Internet. El estado actual, al 01 de enero de 2016, del espacio de direcciones IPv4 totales se indica en la Figura 1.3.

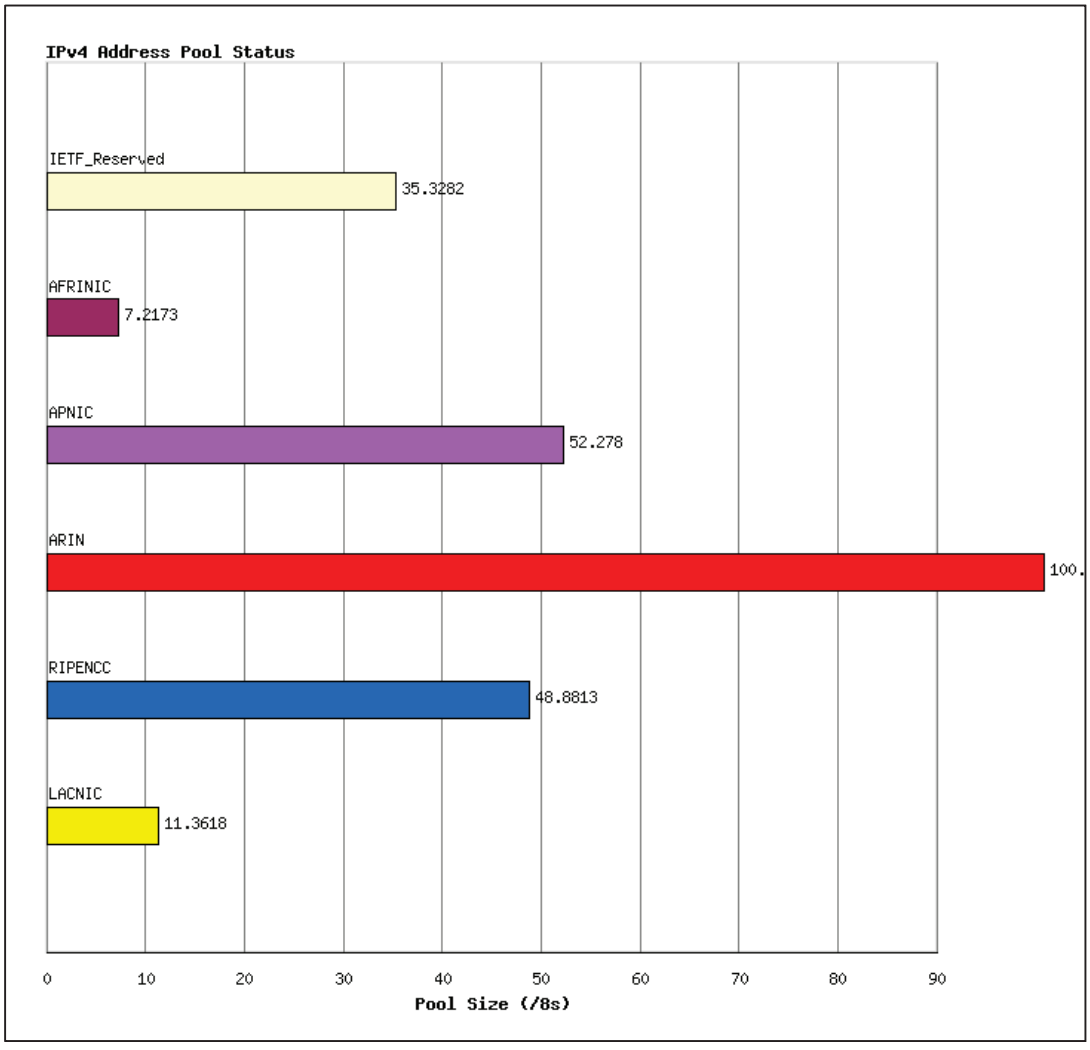


Figura 1.3 Distribución actual de bloques /8 *[8]*

En la Figura 1.3 se observa que la mayor parte de los bloques se encuentra asignado al registro regional ARIN (100 bloques), que distribuye direcciones a Canadá, EE.UU. e islas del noratlántico.

LACNIC tiene al 1 de enero de 2016, 11,3618 bloques /8 disponibles para su uso.

Dentro de los grupos reservados, se encuentran los bloques asignados a direcciones IP privadas, tráfico *"multicast*" y otros usos aún no definidos.

El pasado 03 de febrero de 2011 se hizo la entrega de los últimos cinco bloques de direcciones IP por parte de IANA, uno por entidad, a cada uno de los cinco Registros Regionales de Internet (RIR) en el mundo.

Para la asignación de todos los bloques, que LACNIC tenía bajo su administración, se establecieron ciertas políticas para asignar los recursos disponibles dentro de la región de América Latina y el Caribe.

Estas políticas están diseñadas con el fin de establecer en fases de agotamiento los recursos IPv4 disponibles, lo que quiere decir que las asignaciones son restringidas en tamaño y periodicidad. Gracias a estas políticas se prevé una mejor administración de recursos para un agotamiento gradual de IPv4, así como también el permitir acceso a nuevos actores que quieran iniciar sus actividades de Internet en un futuro.

Agotamiento hace referencia a que LACNIC no va a tener suficientes direcciones para cubrir las necesidades de direccionamiento IPv4 de todos sus miembros.

La finalización del protocolo IPv4 comprende 4 etapas fundamentales los cuales se detallan a continuación:

- *Fase 0:* Todo el espacio disponible hasta llegar al último /9.
- *Fase1:* Desde el último /9 hasta alcanzar los 2 últimos /11 reservados para la terminación gradual de IPv4 y para nuevos entrantes.
- *Fase 2* (Fase Actual): Cuando se alcance el último bloque /10.
- *Fase 3:* Cuando se agote el bloque /11 de terminación gradual.

El manejo de solicitudes de la “Fase 0” se realiza de la siguiente manera: Todas las solicitudes (nuevas y existentes) son tratadas en el orden de llegada mediante un sistema de tickets y el solicitante tendrá un periodo máximo de 30 días para enviar la documentación necesaria, como pagos, acuerdos, contratos, etc., después del cual, se revocará la solicitud y se deberá empezar un nuevo proceso. En esta fase podrían existir excepciones respecto a cambios o aumento de direcciones en solicitudes ya solicitadas. Los nuevos espacios requeridos no necesariamente deben entregarse en un solo bloque, sino que pueden recibir en varios bloques más pequeños hasta alcanzar en sumatoria el bloque solicitado.

El manejo de solicitudes de la “Fase 1” es igual al que se realiza en la “Fase 0” a diferencia de que el periodo máximo para el envío de documentos es de 14 días.

Los nuevos espacios requeridos se pueden entregar en varios bloques más pequeños hasta alcanzar en sumatoria el bloque solicitado, si con la sumatoria no alcanza el bloque requerido, hay dos opciones:

1. Aceptar toda la sumatoria de bloques disponibles.
2. Esperar a que todos los bloques se acaben y realizar la solicitud cuando se ingrese a la “Fase 2”.

El manejo de solicitudes de la “Fase 2” se realiza de igual manera que la “Fase 1” a diferencia que las nuevas solicitudes pueden ser recibidas máximo cada 6 meses. Las asignaciones son de máximo un /22 y mínimo un /24

El manejo de solicitudes de la “Fase 3” se realiza de la siguiente manera: Todas las solicitudes (únicamente nuevas) son tratadas en el orden de llegada mediante un sistema de tickets y el solicitante tendrá un periodo máximo de 14 días para enviar la documentación necesaria, como pagos, acuerdos, contratos, etc., después del cual, se revocará la solicitud y se deberá empezar un nuevo proceso. Las asignaciones son de máximo un /22 y mínimo un /24,

En esta fase, al llegar a uno de los 2 bloques /11, se activa la política de transferencia de recursos [9].

1.3 EL PROTOCOLO IPv6

El protocolo IPv6 comenzó a desarrollarse en el año 1990, tras la primera voz de alerta sobre el posible agotamiento de direcciones IP. Se creó un grupo de trabajo al interior de la IETF (*Internet Engineering Task Force*), quienes presentaron sus primeras recomendaciones sobre el nuevo protocolo que debería reemplazar a IPv4. En el mismo año se publicó oficialmente la primera versión del protocolo IPv6.

El principal motivo por el cual la IETF ve la necesidad de crear y adoptar un nuevo protocolo que reemplace a IPv4, fue la evidente falta de direcciones IPv4.

A diferencia de IPv4 que proporciona 4.294.967.296 direcciones diferentes, IPv6 ofrece un espacio de direccionamiento de 128 bits, esto es 2^{128} que equivale a 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones públicas diferentes.

Los creadores de IPv4 nunca predijeron el *boom* que tendría este protocolo en tan poco tiempo, en una gran variedad de campos, no solo científicos y de educación, sino también en incontables facetas de la vida cotidiana.

Fue a partir de ese momento y debido a la variedad de aplicaciones en las que IPv4 ha sido utilizado, que se ha visto necesario crear “extras” al protocolo básico, éstos son: Calidad de Servicio (QoS), Seguridad (IPsec)[3] y Movilidad[4], entre otros.

El principal inconveniente de estos añadidos de IPv4 es que fueron diseñados posteriormente y es difícil de usar más de un extra simultáneamente.

Para conseguir cubrir las demandas actuales y futuras, las capacidades clave que se buscó con IPv6 son:

- En primer lugar, cualquier nueva versión de IP debía ser capaz de coexistir e inter-operar con las especificaciones actuales de IP. Caso contrario los intentos de una conversión desde una versión hasta la siguiente serían

[3] RFC2401 – *Security Architecture for the Internet Protocol* (IPsec)
[4] *Draft-ietf-mobileip-IPv6-24.txt Mobility Support in IPv6*

irreales y caóticos. Por tanto, IPv6 debía disponer de mecanismos para la comunicación tanto con *hosts* con IPv6 como con *hosts* con IPv4.

- IPv6 debía admitir un espacio de direccionamiento exponencialmente mayor que IPv4.
- Los paquetes de IPv6 debían ser lo más ligeros posibles para facilitar la transmisión de IPv6 por distintos medios.
- Se debía incorporar a IPv6 la Calidad de servicio, QoS (*Quality of Service*), es decir, la capacidad de asignar prioridad y ancho de banda al tráfico y acomodar la funcionalidad que requieren las aplicaciones con baja latencia.
- Los mecanismos de transmisión segura de datos debían ser inherentes a la estructura de IPv6.

Con la perspectiva de las necesidades futuras, y conscientes de temas pasados, el grupo de trabajo de IPv6 del IETF ha creado este nuevo protocolo que presenta más ventajas que la versión anterior.

1.3.1 CARACTERÍSTICAS PRINCIPALES DE IPv6

Entre las principales características que IPv6 presenta se pueden destacar las siguientes:

- **Mayor número de direcciones:** El tamaño de una dirección aumenta desde 32 a 128 [bits] lo que se traduce en alrededor de $3{,}4 \cdot 10^{38}$ direcciones disponibles. Esto permite asegurar que cada dispositivo conectado a una red pueda contar con una dirección IP pública.
- **Nuevo protocolo para interactuar con vecinos:** El protocolo de descubrimiento de vecinos, reemplaza a los protocolos ARP y "*Router Discovery*" de IPV4. Una de sus mayores ventajas es que elimina la necesidad de los mensajes de tipo "*broadcast*".

- ***Plug & Play*: Autoconfiguración:** IPv6 incorpora un mecanismo de auto configuración de direcciones, "*stateless address configuration*", mediante el cual los nodos son capaces de auto asignarse una dirección IPv6 sin intervención del usuario.

- **Nuevo formato de cabecera:** Aun cuando el tamaño de la cabecera en IPv6 es mayor que en IPv4, el formato de ella se ha simplificado. Se han eliminado campos que en la práctica eran poco utilizados, de forma de hacer más eficiente el manejo de los paquetes. Con la incorporación de cabeceras adicionales, IPv6 permite futuras expansiones.
- **Direccionamiento jerárquico:** Las direcciones IPv6 globales están diseñadas para crear una infraestructura eficiente, jerárquica y resumida de enrutamiento basada en la existencia de diversos niveles de ISP. Esto permite contar con tablas de enrutamiento más pequeñas y manejables.

1.3.2 LA CABECERA IPv6

En la Figura 1.4 se muestra la descripción de la cabecera de un paquete IPv4, en la que se ha marcado, mediante el color de fondo, los campos que van a desaparecer en IPv6, y los que se modificarán, según el diseño de la Figura 1.5.

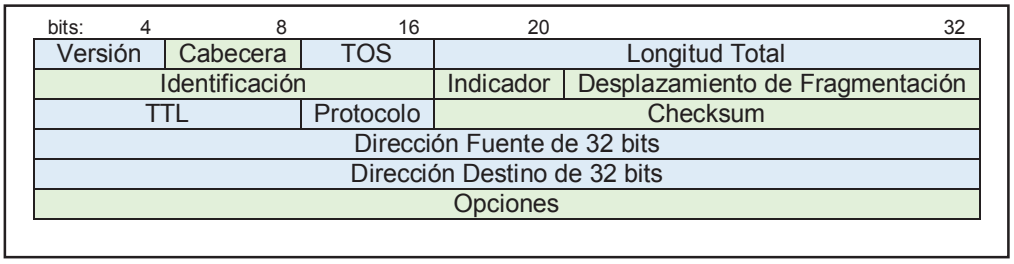


Figura 1.4 La cabecera IPv4

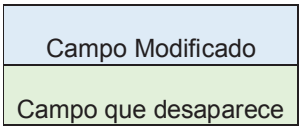


Figura 1.5 Campos modificados y que desaparecen

El principal motivo por el cual los campos son eliminados es por la redundancia que presentaba IPv4, por ejemplo se dispone del campo de *Checksum* o verificación de la integridad de la cabecera en donde esta información también se la puede disponer en otros mecanismos de encapsulado como ATM, PPP, entre otros.

En el caso del campo de "Desplazamiento de Fragmentación" se modifica ligeramente debido a que la forma en la que se realiza la fragmentación de los paquetes es modificada en IPv6, lo que conlleva a la desaparición de este campo. Cuando se utiliza IPv6, los ruteadores o encaminadores no fragmentan los paquetes sino que este trabajo (fragmentación / desfragmentación) es realizado de extremo a extremo.

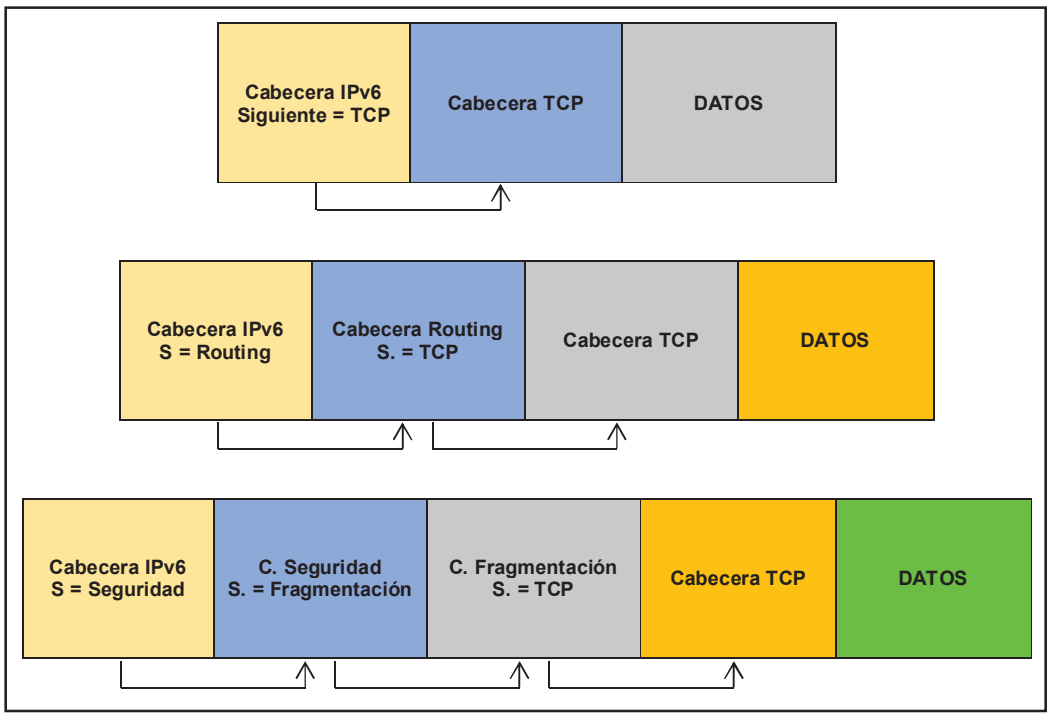


Figura 1.6 Extensiones en IPv6

Algunos campos han sido renombrados, quedando de la siguiente manera:

- El campo "Longitud Total" es renombrado por "longitud de carga útil" (*Payload Length*) y representa la longitud de los datos que puede ser hasta de 65.536 bytes, ya que la longitud de este campo es de 2 bytes (16 bits).

- El campo “Protocolo” es renombrado por “Siguiente Cabecera” (*Next Header*), debido a que en vez de usar cabeceras de longitud variable se utilizan sucesivas cabeceras encadenadas, como muestra la Figura 1.6, y por tal motivo desaparece el campo de opciones. Este campo en la mayoría de casos no es procesado por los ruteadores, sino que tiene un uso extremo a extremo. Su longitud es de 1 byte (8 bits).

- El campo “Tiempo de Vida” es renombrado por “límite de saltos” (*Hop Limit*) el cual presenta una longitud de 1 byte (8 bits).

- El campo “Clase de tráfico” (*Traffic Class*) es renombrado por “Prioridad” (*Priority*) o simplemente “Clase” (*Class*) el cual se asemeja al campo TOS en IPv4. Su longitud es de 1 byte (8 bits).

Se crea el campo “Etiqueta de Flujo” (*Flow Level*) lo que permite indicar que los paquetes pertenecen a determinado “flujo” de tráfico, de esta forma se permite manejar QoS y la administración de ancho de banda sin tener que analizar cabeceras TCP ni UDP. También se han introducido extensiones que permiten autenticación, asegurar la integridad de los datos y cifrado de paquetes opcionales. Este campo tiene una longitud de 2 y medio bytes (20 bits).

De acuerdo a estas modificaciones la cabecera IPv6 queda como se muestra en la Figura 1.7.

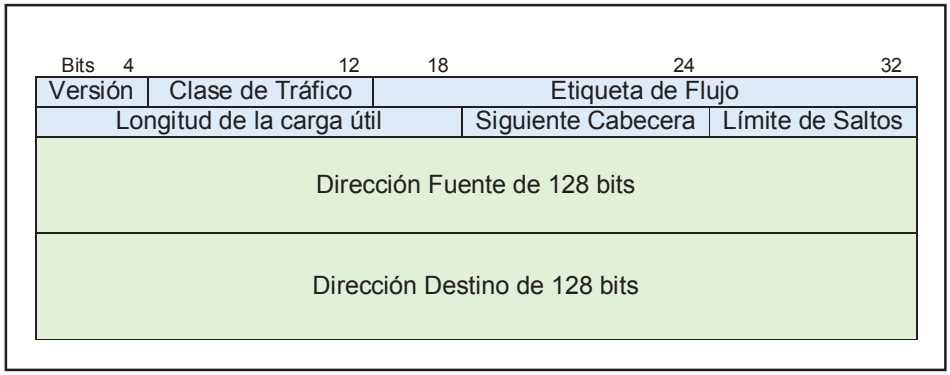


Figura 1.7 Cabecera IPv6

La longitud de esta cabecera es de 40 bytes, el doble de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

La descripción de los campos IPv6 se presentan en la Tabla 1.4.

Después de la cabecera IPv6, puede existir una o más cabeceras de extensión, que son utilizadas para adicionar información sobre el paquete como: información de enrutamiento, el siguiente salto de la ruta indicada por el emisor y también si el paquete se ha fragmentado o no.

Ningún nodo debe procesar estas cabeceras a excepción de la cabecera "*Opciones de Salto a Salto*" que lo hará el nodo destino especificado en el paquete. Las cabeceras de extensión tienen un tamaño múltiplo de 8 bytes.

Tabla 1.4 Descripción de los campos IPv6

Nombre del campo	Tamaño (bytes)	Descripción
Versión	½ (4 bits)	**Versión:** 0110 indica versión 6
Clase de Tráfico	1 (8 bits)	**Clase de Tráfico:** Se usa para identificar la "clase" del tráfico, o la prioridad, de forma que los paquetes se puedan reenviar con distintas prioridades para asegurar la QoS.
Etiqueta de Flujo	2 ½ (20 bits)	**Etiqueta de Flujo:** Los paquetes que pertenecen a un flujo de clase de tráfico concreto se etiquetan para identificar a qué "flujo" pertenecen.
Longitud de la carga útil	2	**Longitud de la carga útil:** Tamaño, en bytes, del resto del paquete, incluyendo las cabeceras de extensión.
Siguiente Cabecera	1	**Siguiente Cabecera:** Identifica el tipo de cabecera que sigue inmediatamente a la cabecera de IPv6. Usa los mismos valores que en el campo Protocolo de IPv4.
Límite de Saltos	1	**Límite de Saltos:** Número de enlaces que puede atravesar un paquete antes de descartarlo. Cada vez que se reenvía este campo se decrementa en uno.
Dirección Origen	16	**Dirección Origen:** Dirección del nodo emisor
Dirección Destino	16	**Dirección Destino:** Dirección del nodo de destino, que puede ser un nodo final o un nodo intermedio.

Los paquetes pueden incluir todas, algunas o ninguna de las cabeceras de extensión de IPv6, pero deberían al menos implementarlas en el orden en el que se relacionan. Cada cabecera de extensión no debería existir más de una vez en cada paquete, a excepción de la cabecera Opciones de destino, que se puede usar una vez para especificar opciones de IP y una segunda vez para especificar opciones de los niveles superiores.

Todas las cabeceras de extensión, de todos los tipos, usan un campo siguiente cabecera, de 8 bits, que especifica el tipo de la siguiente cabecera a la actual. Si este campo contiene el valor “59”, indica que no existen más cabeceras.

- **Cabecera Opciones salto a salto.** Todos los nodos de la ruta de envío deben examinar la cabecera “Opciones salto a salto”. Esta cabecera puede contener varias opciones, que se deben procesar en orden, donde se definen acciones que ocurren en los saltos intermedios en la ruta. El campo “Siguiente Cabecera” identifica la cabecera que sigue a ésta, como se ha mencionado anteriormente.

  El campo “Tamaño de la Cabecera de Extensión” especifica el tamaño de esta cabecera en bytes. El campo “Tipo de Opción”, de 8 bits, especifica la acción que debe tomar un nodo si no se reconocen las opciones del paquete. Como indica este identificador, el nodo puede descartar el paquete, saltar la opción y continuar con el resto de la cabecera o enviar un mensaje “Tipo de Opción” no reconocida de ICMP a la dirección de origen.

- **Cabecera Opciones de destino.** La cabecera “Opciones de Destino” es casi idéntica a la cabecera “Opciones Salto a Salto”, excepto que sólo se examina en el nodo de destino del paquete y no en los nodos intermedios de la ruta. El valor “60” en el campo “Siguiente Cabecera” de la cabecera anterior indica la presencia de la cabecera “Opciones de Destino”. El resto de campos son idénticos a los de Opciones salto a salto.

- **Cabecera Enrutamiento.** En IPv6, un nodo de origen puede listar una o más paradas (*stop*) en la ruta del paquete. La cabecera “Enrutamiento” no se examina hasta que el paquete alcanza el destino de la cabecera de IPv6. A

continuación, en el destino se examina la cabecera “Enrutamiento”, se procesa de acuerdo al algoritmo indicado en el campo “Tipo de Enrutamiento”, y se usa el resultado para enviar el paquete a la dirección del siguiente destino especificada en el paquete.

El campo de 8 bits “Segmentos Restantes” indica el número de direcciones que quedan por visitar, y el campo de 32 bits “Reservado” se pone a cero y se ignora en la transmisión. Según se va enviando el paquete a cada nodo especificado en la cabecera de “Enrutamiento”, las direcciones visitadas se eliminan del paquete y se decrementa la cuenta de saltos, hasta que eventualmente el paquete llega a su destino final.

- **Cabecera Fragmentación.** IPv6 requiere una MTU de enlace mínima de 1.280 bytes. En IPv6, el nodo de origen realiza la fragmentación, no los enrutadores. Sin embargo, la presencia de una cabecera Enrutamiento puede requerir que los nodos intermedios fragmenten el paquete como resultado de una MTU distinta en la ruta. Como cada uno de los saltos se convierte en nodo de origen según se envía el paquete a la siguiente dirección, al nodo sólo le interesa la MTU del enlace entre el mismo y el destino, en lugar de conocer la MTU de todos los enlaces de la red.

  El campo “Desplazamiento de Fragmentación” determina el orden de re-ensamblado en el nodo de destino y a cada fragmento se le asigna un valor único en el campo Identificación para facilitar la retransmisión de paquetes perdidos. Un indicador M de valor “0” indica que éste es el último de los fragmentos y un valor de “1” indica que existen más fragmentos a continuación.

- **Cabecera Autenticación.** La cabecera Autenticación se usa por sí misma o junto a las cabeceras ESP (*Encapsulating Security Payload*), para proporcionar verificación del origen de los datos. Sin embargo, la cabecera Autenticación no proporciona cifrado de datos; en IPv6 es responsabilidad de ESP.

El campo “Tamaño de los Datos”, de 8 bits, de la cabecera Autenticación especifica el tamaño de la cabecera en palabras de 32 bits.

El campo Reservado, de 16 bits, no se usa actualmente y se debe fijar en “0”.

El campo Índice de parámetros de seguridad, SPI (*Security Parameters Index*), es un valor arbitrario de 32 bits. Junto con la dirección del nodo de destino y el protocolo de seguridad negociado entre ambos nodos, este valor identifica unívocamente la asociación de seguridad del paquete.

El campo “Número de Secuencia” se incrementa en 1 con cada paquete y no se permite que este contador dé la vuelta sin que los nodos emisor y receptor establezcan una nueva asociación de seguridad. El tamaño de los datos de autenticación es variable, pero debe ser un múltiplo de 32 bits y se rellena con lo necesario para cumplir con este requisito.

- **Mecanismos de transición.** Los mecanismos para la transición de IPv4 a IPv6 se definen en el RFC 1933. El objetivo principal del proceso de transición es la coexistencia de las dos versiones de los protocolos hasta que IPv4 desaparezca completamente en algún momento. Los planes de transición constan de dos categorías principales: la implementación de pilas duales y el túnel de IPv6 sobre IPv4.

1.3.3 DIRECCIONAMIENTO EN IPv6

Las direcciones IPv6[5] son identificadores de 128 bits de longitud e identifican interfaces de red (ya sea de forma individual o grupos de interfaces). A una misma interfaz de un nodo se le pueden asignar múltiples direcciones IPv6. Dichas direcciones se clasifican en tres tipos:

[5] RFC2373 – IP *Version 6 Addressing Architecture*

1. ***Unicast*:** Identificador para una única interfaz. Un paquete enviado a una dirección *unicast* es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

2. ***Anycast*:** Identificador para un conjunto de interfaces (normalmente pertenecen a diferentes nodos). Un paquete enviado a una dirección *anycast* es entregado en una de las interfaces identificadas con dicha dirección (a cualquiera que esté más "cerca"). Permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el *routing*), si la primera "cae".

3. ***Multicast*:** Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección *multicast* es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (*broadcast*).

Según el estándar RFC 3177, la asignación recomendada será de la siguiente manera:

- Asignar un prefijo /32 a ISP o LIRs (*Local Internet Registry*) con lo cual el número de direcciones disponibles sería 2^{96}.

- Asignar un prefijo /48, para el caso general (Organización), excepto para los subscriptores muy grandes, con lo cual en número de direcciones disponibles sería 2^{80}.

- Asignar un prefijo /64, para alguna red de alguna organización, con lo cual se tendrían 2^{64} direcciones disponibles. **Ésta será la unidad mínima que se manejará en los planes de numeración.**

- Asignar un prefijo /128, cuando sólo existe un único *host* conectado (PC, servidor, Impresora, *router*).

1.3.3.1 Direcciones *unicast* IPv6

Las direcciones *unicast* tienen la función de individualizar a cada nodo conectado a una red, lo que permite brindar conexión punto a punto entre nodos de la misma red. Un aspecto que se introduce en IPv6 es el uso de contextos en las direcciones *unicast*. Los contextos identifican el dominio de una red, ya sea lógico o físico. El objetivo de poder manejar contextos es el de optimizar el desempeño de la red. Las direcciones IPv6 pueden pertenecer a uno de los siguientes 3 contextos:

1. Local al enlace ("*link-local*"): Identifica a todos los nodos dentro de un enlace o red.

2. Local único ULA ("*unique-local*"): Identifica a todos los dispositivos dentro de una red interna o sitio, compuesta por varios enlaces o dominios de capa 2.

3. Global: Identifica a todos los dispositivos ubicables a través de Internet.

Estos contextos presentan un orden jerárquico tal como se muestra en la Figura 1.8.

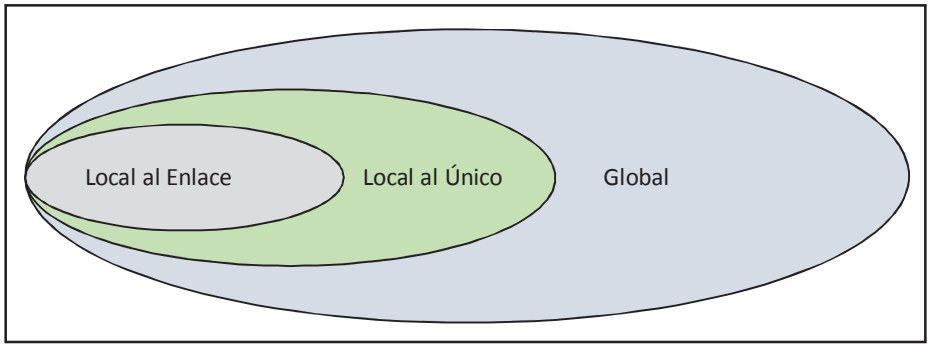


Figura 1.8 Contextos de Direcciones *Unicast*

Una Interfaz puede tener más de una dirección IPv6. Por ejemplo, un nodo puede contar con una dirección *Link Local* para comunicarse con los dispositivos locales y una o más direcciones globales para comunicarse hacia el Internet.

1.3.3.1.1 Direcciones unicast IPv6 Link Local (FE80::/10)

Las direcciones *Link Local* solo pueden usarse en el ámbito de un enlace y siempre estarán presentes en la interfaz con IPv6 activado. Una manera de ver si se dispone de soporte IPv6 en un dispositivo o una interfaz, es verificando si se tiene una dirección *Link Local*.

En la práctica se compone del prefijo FE80::/64 + los 64 bits de menor peso llamados identificadores de interfaz que se generan localmente en el *host*, ya sea a partir de su dirección MAC, de manera aleatoria (RFC 4941), por medio de DHCPv6 o manualmente.

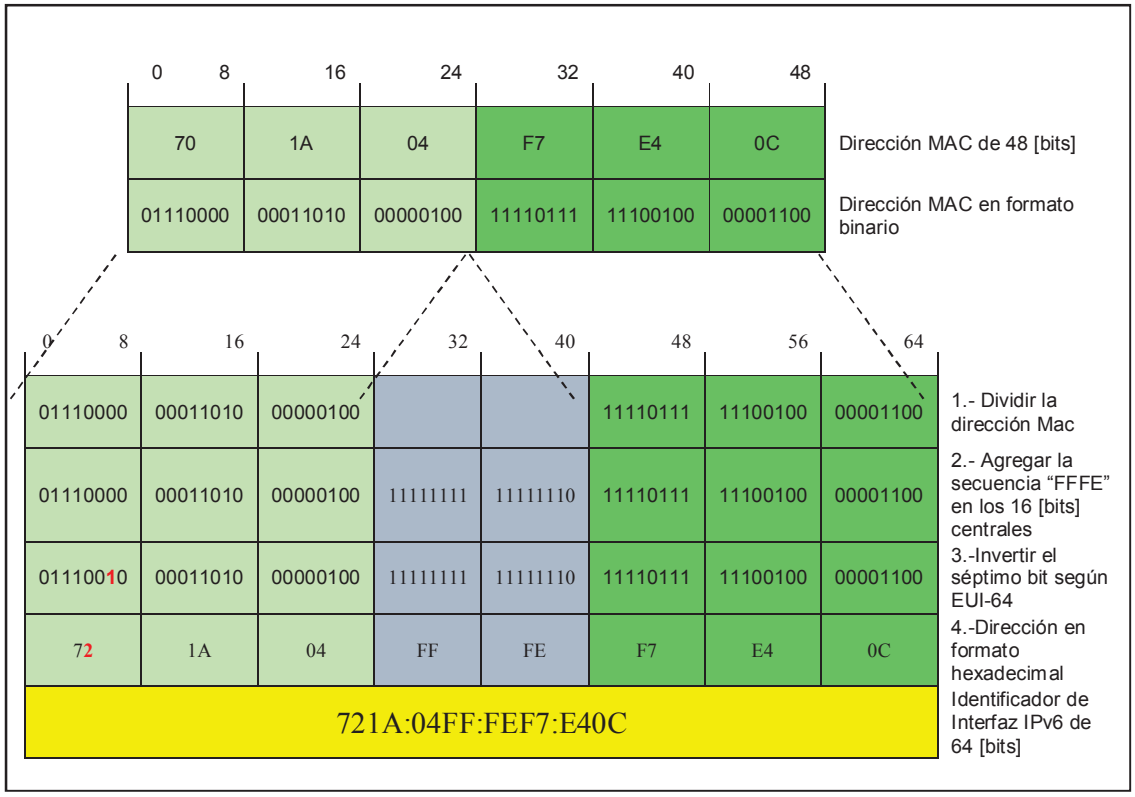


Figura 1.9 Creación del Identificador de Interfaz

Cada vez que un nodo IPv6 se conecta a una red, adquiere de forma automática una dirección *Link Local* sin necesidad de que ésta tenga que ser configurada manualmente.

La estructura de una dirección *Link Local* es “FE80:0:0:0:<identificador de interfaz>”“. El identificador de interfaz se genera automáticamente a partir de su dirección MAC, siguiendo el formato EUI-64[6] [10]. En la Figura 1.9 se detalla cómo se construye el identificador de interfaz IPv6 a partir de la dirección MAC.

Como ejemplo se trabajará con la dirección MAC 70:1A:04:F7:E4:0C

La dirección *Link Local* quedaría de la siguiente manera: FE80:0000:0000:0000:721A:04FF:FEF7:E40C en formato completo ó FE80::721A:04FF:FEF7:E40C en formato comprimido.

Las direcciones *Link Local* permiten la conectividad rápida y simple entre nodos conectados a un mismo enlace, con lo cual no dependerán de prefijos IPv6 anunciados en la red y se podrá identificar directamente a nodos y *routers* presentes en el enlace.

1.3.3.1.2 Direcciones unicast IPv6 locales únicas ULA (FC00::/7)

Las direcciones ULA se han definido para ser usadas dentro de un sitio (red organizacional, de prefijo /48, compuesta por una o más subredes) y tienen el formato mostrado en la Figura 1.10. El prefijo FC00::/7 va seguido de un bit “L” que valdrá “1” si el prefijo es creado localmente por una organización, y “L” valdrá “0” cuando en un futuro, según el RFC 4193, alguna organización asignare de manera centralizada este tipo de prefijos. A continuación habrá el componente aleatorio de 40 bits, cuyo objetivo es hacer altamente improbable que exista otro prefijo ULA idéntico en otro sitio.

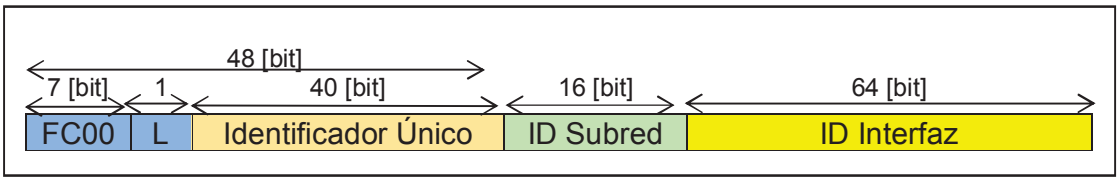


Figura 1.10 Estructura de una Dirección Local Única

[6] RFC 4291: *IP Version 6 Addressing Architecture*

De esta manera se crea un prefijo /48, que si L=0, comenzará por FD00::/8

Las direcciones ULA son el equivalente a las direcciones privadas en IPv4[7], cuya función es proveer conectividad entre los nodos de un sitio o intranet[8] [11]. De igual manera que las direcciones *Link Local*, éstas no pueden ser enrutadas hacia Internet. Su estructura se detalla en la Figura 1.10.

Todas las direcciones locales únicas se encuentran dentro del rango dado por el prefijo FC00::/7. Los campos de una dirección *unicast* local única son:

- **Identificador Único:** Identifica a un sitio en particular. Dado que este tipo de direcciones no son publicadas en Internet, pueden existir distintos sitios con el mismo identificador.
- **Identificador Subred:** Permite crear un plan de direccionamiento jerárquico, identificando a cada una de las 2^{16} posibles subredes en un sitio.
- **Identificador de Interfaz:** Individualiza a una interfaz dentro de una determinada subred del sitio. A diferencia de las direcciones *Link Local*, este identificador **no** se genera automáticamente.

1.3.3.1.3 Direcciones unicast IPv6 globales GUA (2000::/3)

Las direcciones *unicast* IPv6 globales se utilizan para comunicar 2 nodos por medio del Internet. Son el único tipo de direcciones que son utilizadas para enrutar tráfico a través de Internet. El espacio que se encuentra reservado para estas direcciones va desde el 2001:: al 3fff:ffff:ffff:ffff:ffff:ffff:ffff (2001::/3).

Todas las subredes en el espacio de direccionamiento *unicast* global tienen un prefijo de red fijo y equivalente a /64[9]. Esto implica que los primeros 64 [bits] (los primeros 4 campos en formato hexadecimal) corresponden al identificador de red,

[7] Bloques 10.X.X.X/8; 172.16.X.X /12; 192.168.X.X /16
[8]Una intranet es una red de ordenadores privados que utiliza tecnología Internet para compartir dentro de una organización parte de sus sistemas de información y sistemas operacionales.
[9] Esta es la norma más usada, pero se pueden usar prefijos más grandes.

y los siguientes corresponden a la identificación de la interfaz de un determinado nodo. En la Figura 1.11 se observa la estructura de una dirección *unicast* global.

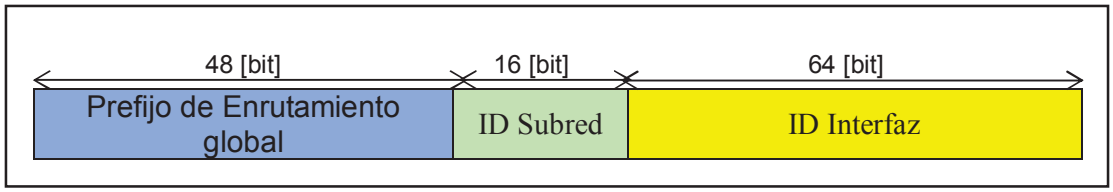


Figura 1.11 Estructura de una dirección *unicast* global

El prefijo de enrutamiento global identifica un sitio que se encuentra conectado a Internet. Dicho prefijo sigue una estructura jerárquica, con el fin de reducir el tamaño de la Tabla de enrutamiento global en Internet. En la Figura 1.12 se presenta la estructura utilizada actualmente para la delegación de prefijos.

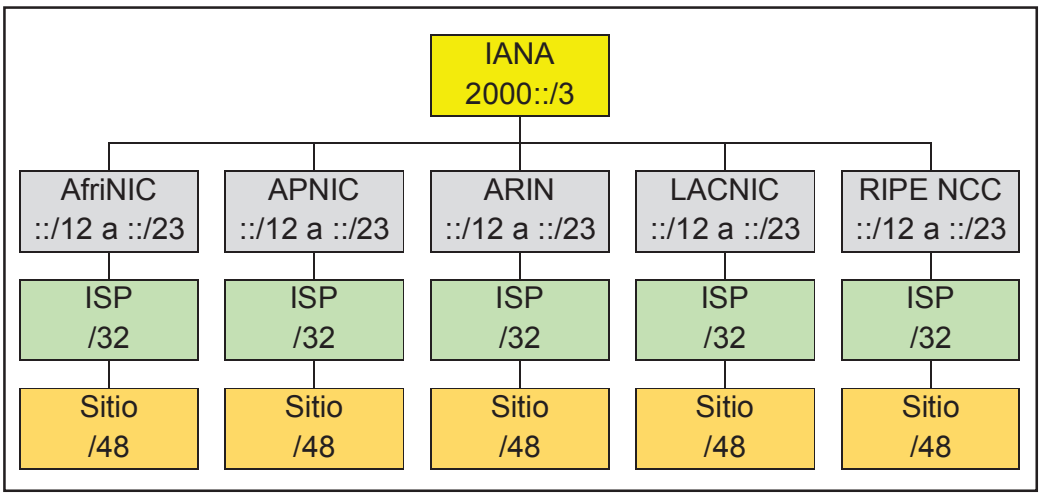


Figura 1.12 Jerarquía de delegación de prefijos *Unicast* Globales

Del espacio total que está asignado por la IANA (2000::/3), cada registro regional (RIR) se le permite manejar prefijos entre ::/12 hasta ::/23, los cuales distribuyen prefijos ::/32 a proveedores de servicios de Internet (ISPs) presentes en cada una de las respectivas regiones. A los usuarios finales se les asigna prefijos /48 otorgados directamente por cada uno de los ISPs, lo que les permite contar con

una intranet compuesta por 2^{16} subredes, cada una con capacidad de conectar hasta 2^{64} dispositivos a Internet.

1.3.3.2 Direcciones *multicast* IPv6 (FF00::/8)

En IPv6 el tráfico *multicast* permite a dispositivos IPv6 ubicados en distintos lugares recibir tráfico dirigido a una única dirección *multicast*, de la misma manera que IPv4. Una dirección *multicast* presenta la estructura mostrada en la Figura 1.13.

Las direcciones *multicast* IPv6 comenzarán con FF, a continuación se definen 4 bits para ser utilizados como *Flags* en el *routing* y servicios *multicast*.

Los cuatro bits siguientes indican el ámbito o "*Scope*" de la dirección, es decir, el área donde esta dirección es válida; se definen los valores mostrados en la Tabla 1.5, siendo los más comunes el 2 (para un enlace), el 5 (para un sitio) y E (para ámbito global).

El identificador de grupo o "*Group ID*" identificará el grupo *multicast* y tiene una longitud de 112 bits.

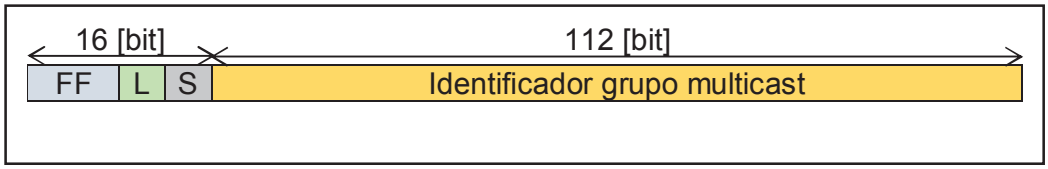


Figura 1.13 Estructura de direcciones Multicast

El campo L indica el tiempo de vida de un grupo *multicast*, tomando el valor de 0 cuando es un grupo permanente y 1 cuando es un grupo *multicast* temporal. El campo S indica el contexto o alcance del grupo, de acuerdo a los valores presentados en la Tabla 1.5.

IPv6 no utiliza direcciones *broadcast*, sino que las sustituye por direcciones *multicast*, lo que permite seleccionar de manera más precisa a los destinatarios de una solicitud, evitando sobrecarga de mensajes en redes con muchos nodos. En la Tabla 1.6 se muestran algunos grupos de direcciones *multicast* existentes.

Tabla 1.5 Código de contextos en una dirección *multicast*

Valor del campo S (hexadecimal de 4 bits	Contexto del grupo
1	Interfaz
2	Enlace
5	Sitio
8	Organización
E	Global
Otros Valores	Sin asignar o reservado

Tabla 1.6 Direcciones fijas de grupos *multicast*

Dirección *Multicast*	Descripción
FF01::1	Todos los nodos en la Interfaz
FF02::1	Todos los nodos en el enlace
FF01::2	Todos los *routers* en la Interfaz
FF02::2	Todos los *routers* en el enlace
FF05::2	Todos los *routers* en el sitio

1.3.3.2.1 Direcciones multicast de nodo solicitado (SN) (FF02:0:0:0:0:1:FF/104)

Otras direcciones que se configuran normalmente en los nodos IPv6 son las *Solicited Node* (SN), que son direcciones *multicast* generadas a partir de las direcciones *unicast* y *anycast* usadas por el nodo. Para ello se concatena el prefijo FF02::1:FF/104 con los últimos 24 bits de la dirección *unicast* o *anycast* asociada.

Si la dirección acaba en: “XX:ZTUV” la SN es: FF02::1:FFXX:ZTUV

Cada nodo IPv6 debe unir la dirección SN a todas sus direcciones *unicast* y *anycast*.

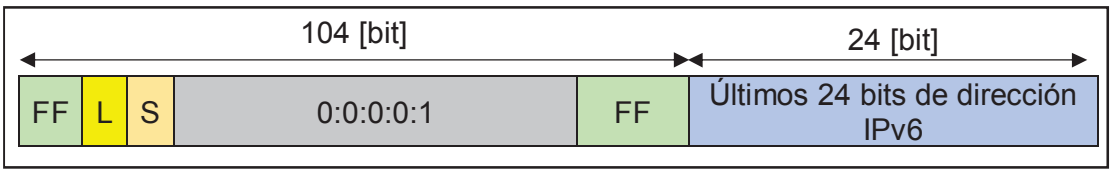


Figura 1.14 Estructura dirección *multicast* de nodo solicitado

Las direcciones *multicast* de nodo solicitado se utilizan para realizar la asociación entre direcciones capa 2 (MAC) y direcciones IPv6. Esta dirección contiene parte

de la dirección IPv6 que se desea consultar y posee la estructura descrita en la Figura 1.14.

Cuando un nodo se configura con una dirección IPv6, automáticamente se une al grupo *multicast* indicado por su dirección de nodo solicitado, debido a que dicha dirección toma solo los últimos 24 bits de la dirección IPv6.

En la Tabla 1.7 se muestran algunas direcciones IPv6 con sus correspondientes direcciones *multicast* de nodo solicitado.

Tabla 1.7 Ejemplos de direcciones *multicast* de nodo solicitado

Dirección IPv6	Dirección *multicast* de nodo solicitado
2800:270:bcd0:3::1	ff02::1:ff00:1
2800:270::1230:1000:a34:9e9a	ff02::1:ff34:9e9a
2800:270::34de:2000:a34:9e9a	ff02::1:ff34:9e9a
fc00:0:0:1::aaaa:a1	ff02::1::ffaa:a1

Cuando un nodo requiere enviar un paquete a un vecino en el mismo enlace y no conoce su dirección física, envía un mensaje que contiene la dirección IPv6 a consultar al grupo *multicast* de nodo solicitado. Todos los nodos que estén en dicho grupo *multicast* reciben el mensaje, pero solo responde el nodo configurado con la dirección IPv6 solicitada.

1.3.3.3 Direcciones *anycast*

Las direcciones *anycast* identifican a un grupo de interfaces. Los paquetes que son enviados a una dirección *anycast* son reenviadas por el dispositivo de enrutamiento hacia la interfaz que se encuentra más cercana al origen del paquete. La entrega del paquete se facilita puesto que el dispositivo de enrutamiento conoce la distancia (métrica) hacia cada uno de los demás dispositivos y las interfaces que están asociadas a cada dirección *anycast*.

Para configurar una dirección *anycast*, basta con configurar una misma dirección *unicast* en distintos dispositivos, y configurar en cada *router* una ruta directa hacia

dicha dirección (/128). Con esto se consigue que cada *router* posea en su tabla de enrutamiento varias entradas hacia la misma dirección, con sus métricas asociadas. Al fallar la ruta más cercana, se selecciona automáticamente la siguiente.

El uso de direcciones *anycast* permite, entre otras cosas, implementar balanceo de carga y tolerancia a fallas. Generalmente se usa en redes locales. Las direcciones *anycast* son válidas únicamente como direcciones de destino para los paquetes IPv6, al igual que las *multicast*.

1.3.4 TIEMPO DE VIDA DE DIRECCIONES IPv6

Las direcciones IPv6 se asignan a una interfaz por un tiempo determinado, que puede ser infinito, e indica el periodo de validez de la asignación.

Se utilizan dos valores de tiempo o 2 temporizadores:

1. *Preferred*
2. *Valid Lifetime*

De forma que la dirección puede estar en 3 estados, según la Figura 1.15.

1. Inicialmente, una dirección es preferida "*Preferred*" mientras los temporizadores *Preferred* y *Valid* siguen activos. Su uso en una comunicación arbitraria no está restringido.

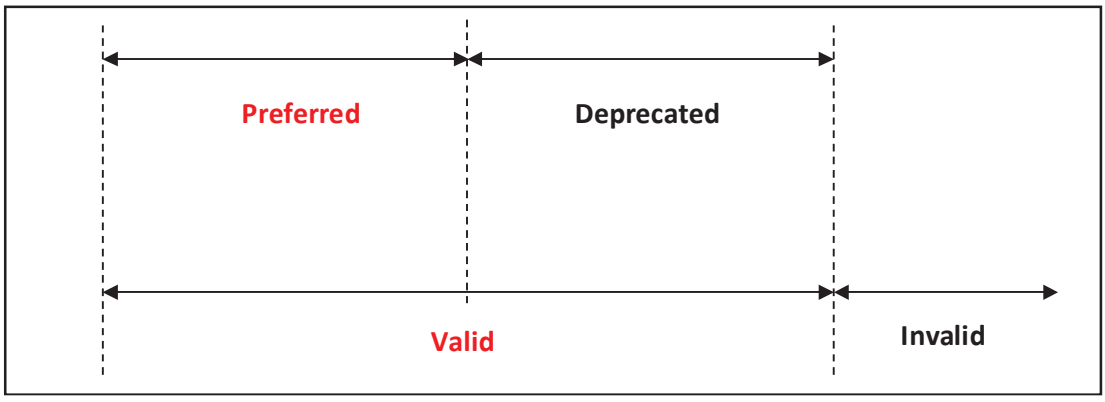


Figura 1.15 Tiempo de vida de direcciones IPv6

2. Cuando expira el temporizador *Preferred*, pero sigue activo el temporizador *Valid*, la dirección se convierte en "*Deprecated*" anticipándose al hecho de que su asignación a la interfaz de red será inválido en instantes. En este estado, esta dirección puede usarse para comunicaciones en curso pero no para nuevas comunicaciones.

3. Cuando también expira el temporizador *Valid*, entonces la dirección es inválida y debe dejarse de usar para cualquier comunicación.

1.3.5 FORMATO DE UNA DIRECCIÓN IPv6

Una dirección IPv6 está compuesta por 8 campos de 16 bits de largo cada uno, separados uno de otros por dos puntos (:); por lo que cada uno de los campos está representado por 4 caracteres hexadecimales [0 – F]. Por ejemplo una dirección IPv6 válida es 2001:1100:1214:2010:0000:C1D0:AF0D:08D6. Con el fin de simplificar la escritura, se pueden aplicar las siguientes reglas a las direcciones IPv6.

- No hay distinción entre mayúsculas y minúsculas. (AFD6) es equivalente a (afd6).

- Los ceros a la izquierda de un campo son opcionales. (00c1) es equivalente a (c1).

- Una sucesión de campos con ceros puede ser reemplazados por (::). (3241:0000:0000:fce4) es igual a (3241::fce4)[10].

De la misma manera que en el caso de IPv4, para señalar las secciones de la dirección que identifican a la red y al dispositivo, se utiliza el formato CIDR[11] en la forma dirección/prefijo. Por ejemplo, una dirección en la forma 3ffe:b00:c18:1::1/64 señala que los primeros 64 [bit] (3ffe:b00:c18:1) identifican a la red y los restantes 64[bit] (::1) identifican al dispositivo de dicha red.

---

[10] Esta regla sólo se puede utilizar una vez en una dirección IPv6, de lo contrario el sistema no sabría cuántos campos se han comprimido en cada caso.

[11] CIDR: *Classless Inter-Domain Routing* (Enrutamiento entre dominios sin Clases)

El uso de los dos puntos (:) en IPv4 representa el puerto de un determinado nodo, por ejemplo 172.196.0.1:80 indica que se usa el puerto 80 (www) del nodo 172.196.0.1. Lo que genera una incompatibilidad entre direcciones IPv4 e IPv6.

La solución a este problema es representar la dirección IPv6 encerrada por corchetes y seguida por los dos puntos (:) y el puerto; de la siguiente manera: [dirección]:puerto como por ejemplo [3ffe:b00:c18:1::1]:80

1.3.6 ESTRATEGIAS DE TRANSICIÓN A IPV6

Se debe tener en cuenta en que se debe buscar la mejor estrategia de transición a IPv6, teniendo en cuenta que va a convivir con IPv4 durante mucho tiempo.

Desde su diseño inicial, IPv6 se creó con la idea de fondo de que debía permitir una transición amigable con IPv4, permitiendo introducir el nuevo protocolo sin interferir con el normal funcionamiento de IPv4; aun así IPv4 a IPv6 son protocolos no compatibles entre sí, es decir, una pila IPv4 no entiende un paquete IPv6 y viceversa.

El objetivo es añadir conectividad IPv6 en las redes, dispositivos, servicios y aplicaciones coexistiendo con IPv4. Actualmente existe un nuevo factor a tener en cuenta, el agotamiento de direcciones IPv4.

Como guías generales para la elaboración de una estrategia de transición hay que tener en cuenta lo siguiente:

- IPv6 coexistirá con IPv4
- Lo recomendable es seguir el esquema ya existente para IPv4
- Tres opciones principales: IPv6 nativo, túneles y traducción

En orden de preferencia las 3 posibles estrategias de transición son:

- **IPv6 nativo**: Se utiliza la cabecera IPv6 del paquete para la transmisión de datos desde el origen al destino final. Existen 2 opciones:

1. *Dual Stack* o Doble Pila: Consiste en tener en los dispositivos ambos protocolos funcionando a la vez, en paralelo.

2. Sólo-IPv6: consiste en usar sólo IPv6 sin IPv4.

- **Túneles**: Consisten en encapsular una versión de IP en otra.

- **Traducción**: Será necesaria para comunicar 2 *host* que solo hablan una versión cada uno y además versiones diferentes de protocolos IP.

1.3.7 MECANISMOS DE TRANSICIÓN (MT) (RFC 1933)

Son técnicas usadas para permitir conectividad IPv6 y, en algunos casos, para mitigar la escasez de IPv4. Son las herramientas usadas por las estrategias de transición.

Los mecanismos basados en túneles se deben usar cuando se quieren enviar paquetes de una versión IP a través de una red que no soporta esa versión, para ello, se encapsula el paquete a enviar en un paquete IP en una versión soportada por la red a atravesar.

Los túneles pueden ser estáticos o automáticos, punto a punto o multipunto; constituyen el mecanismo de transición más común.

Se pueden encapsular IPv6 en IPv4 directamente, se puede utilizar una cabecera GRE (*Genereric Routing Encapsulation* - RFC2784) o usar UDP (*User Datagram Protocol* – RFC 768) para atravesar NAT (*IP Network Address Translator* – RFC 2663) o incluso encapsular IPv4 en IPv6 como se muestra en la Figura 1.16.

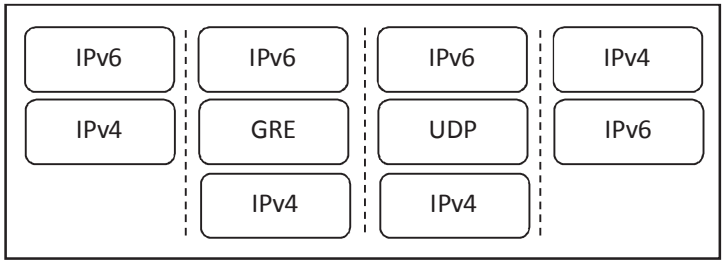


Figura 1.16 Mecanismo de Transición por Túneles

Los mecanismos de traducción son los menos recomendados pero son la única opción cuando se quiere comunicar un *host* que solo entiende una versión del protocolo con otro *host* que solo entiende la otra versión del protocolo IP. Para ello hace falta un elemento traductor entre los dos tipos de redes.

Según quien inicie la comunicación se tendrá comunicación desde un *host* sólo IPv6 hacia un *host* sólo IPv4 o desde un *host* sólo IPv4 a un *host* sólo IPv6, esta última opción se considera OBSOLETA (RFC4966) y no se recomienda, no existen estándares ni implementaciones para lograr esto. Si se quiere comunicar un *host* sólo IPv4 con un *host* sólo IPv6 se debe ofrecer conectividad IPv6 al *host* sólo IPv4.

1.3.7.1 IPv6 Nativo

La opción recomendada a la hora de llevar a cabo la transición a IPv6 es IPv6 Nativo, sin encapsular, ni traducir los paquetes. Los paquetes IPv6 Nativo circularán por la red desde el origen hasta el destino utilizando la cabecera IPv6 para el *routing* y el resto de servicios de la capa IP.

La principal ventaja de esta estrategia es que el esquema, configuración, direccionamiento, monitorización, queda establecido para IPv6 de manera definitiva, no queda pendiente de posteriores cambios o mejoras para que el tráfico IPv6 funcione de manera nativa. Se puede decir que se lleva a cabo una implementación en un solo paso, al contrario que con el uso de mecanismos de transición basados en túneles o traducción, que serán temporales y necesitarán un paso añadido en el que se eliminen estos mecanismos.

Por otro lado, requiere que todos los elementos involucrados en el tráfico de paquetes soporten IPv6, lo que no siempre ocurre. Se tienen dos opciones a la hora de implementar IPv6 Nativo.

- Doble Pila (*Dual Stack*) donde se utilizan a la vez IPv4 e IPv6
- Sólo IPv6 (*IPv6-only*), de forma que solo se use IPv6 en la red

1.3.7.1.1 Doble Pila o Dual Stack

La opción de Doble Pila, consiste en habilitar IPv4 e IPv6 a la vez en los dispositivos de red, de forma, que por la misma pila de red, interfaz y el mismo cable, circulen a la vez los paquetes IPv4 e IPv6 nativo.

La ventaja de esta aproximación es que IPv4 seguirá funcionando al igual que antes, sin verse afectado, y se podrá llevar a cabo una introducción gradual de IPv6 ahí donde se pueda.

El comportamiento habitual es el de dar preferencia a IPv6 sobre IPv4 cuando ambos están disponibles. A lo largo del tiempo ha habido un cambio sobre estas preferencias por defecto en los sistemas operativos. Inicialmente se daba preferencia a todo el IPv6, ya fuera nativo o por mecanismos de transición, sobre IPv4. Se vio que podría dar problemas si el mecanismo de transición daba un mal servicio IPv6, por lo que actualmente en la recomendación es dar preferencia a IPv6 nativo, seguido de IPv4 nativo y por último IPv6 mediante mecanismos de transición, según muestra la Figura 1.17.

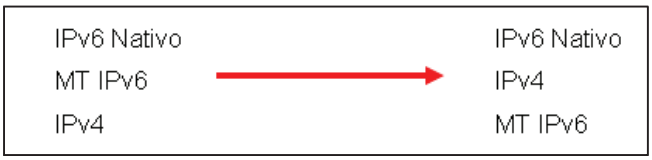


Figura 1.17 Preferencias de IPv6 en sistemas Operativos

El hecho de coexistir IPv4 sobre IPv6 tiene implicaciones distintas según se lo vea desde el plano de datos o desde el plano de control o gestión.

Desde el plano de datos, el tráfico que pase a ser IPv6, dejará de existir en IPv4, es decir, no se añade o suma tráfico IPv6 al que ya se contaba con IPv4. Por ejemplo, si se ve un video de YouTube en IPv6, se deja de hacerlo sobre IPv4. En este escenario, el ancho de banda ocupado por la infraestructura no debe aumentar por utilizar IPv6.

Desde el plano de gestión o control, se deben aumentar los recursos ya que habrá más complejidad de red, doble espacio de direccionamiento, doble protocolo de *routing* (IPv4 e IPv6), doble configuración, doble control de seguridad, etc.

Como se muestra en la Figura 1.18, un servicio (service.example.com) disponible en un servidor de Doble Pila, puede ser accedido desde cualquier tipo de *host*, ya sea, sólo-IPv4, sólo-IPv6 o Doble Pila utilizando cualquiera de las versiones del protocolo. Lo que se hace es publicar en el DNS, las direcciones IPv4 e IPv6 que el cliente obtendrá por DNS, y decidirá cuál utilizar. Por defecto, se da preferencia en la mayoría de los casos a IPv6.

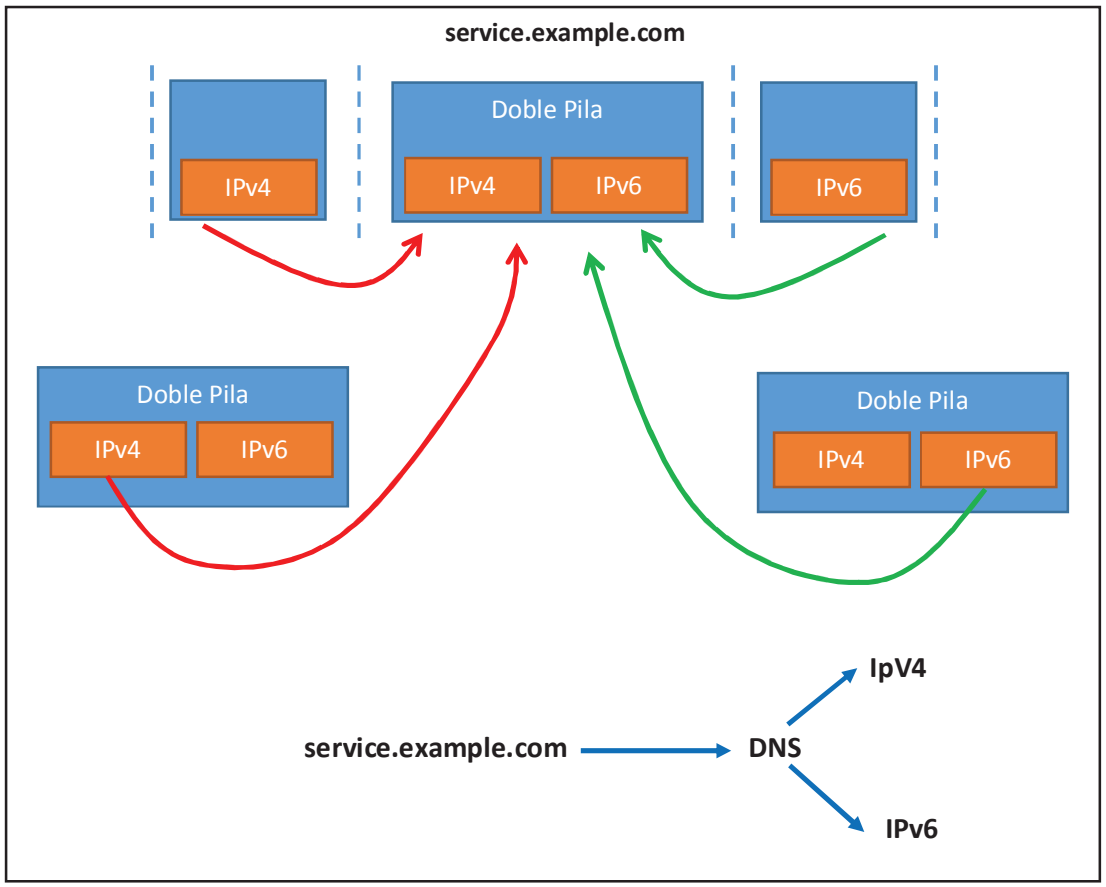


Figura 1.18 Funcionamiento Servicio Doble Pila

En la Figura 1.19 se muestra un ejemplo de configuración de una interfaz eth0 en un sistema operativo Linux. En esta interfaz se configura tanto IPv4 como IPv6, de

forma que tendrá direcciones IPv4 e IPv6 a la vez y aceptará tráfico de ambos protocolos.

```
auto eth0
iface eth0 inet static
        address 10.0.0.10
        netmask 255.255.255.0
iface eth0 inet6 static
        address 2001:db8:1234:5::1:1
        netmask 64

#ifconfig -> para Verificar
eth0    Link encap:Ethernet     HWaddr 00:E0:81:05:46:57
        inet addr:10.0.0.10     Bcast:10.0.0.255        Mask:255.255.255.0
        inet6 addr: fe80::2e:81ff:fe05:4657/64  Scope:Link
        inet6 addr: 2001:db8:1234:5::1:1/64     Scope:Global
        UP BROADCAST RUNNING MULTICAST  MTU:1500        Metric:1
        RX packets:2010563 errors:0 dropped:0 overruns:0 frame:0
        TX packets:1700527 errors:0 dropped:0 overruns:2 carrier:0
        collisions:0 txqueuelen:100
        RX bytes:205094215 (195.5 Mb) TX bytes:247063610 (235.6 Mb)
        Interrupt:11 Base address:0xe000 Memory:f8201000-f8201038
```

Figura 1.19 Configuración Interfaz eth0 en Linux

El hecho que se de preferencia a IPv6 por defecto y de manera estática, se comprobó que puede dar lugar a situaciones problemáticas.

```
     DNS SERVER                      Cliente                          Server
        |                              |                               |
1.      |<--www.example.com     A?-----|                               |
2.      |<--www.example.com     AAAA?--|                               |
3.      |---192.0.2.1----------------->|                               |
4.      |---2001:db8::1--------------->|                               |
5.      |                              |                               |
6.      |                              |==TCP  SYN,    IPv6===>X       |
7.      |                              |==TCP  SYN,    IPv6===>X       |
8.      |                              |==TCP  SYN,    IPv6===>X       |
9.      |                              |                               |
10.     |                              |--TCP  SYN,    IPv4---------->|
11.     |                              |<-TCP  SYN+ACK,        IPv4----|
12.     |                              |--TCP  ACK,    IPv4---------->|
```

Figura 1.20 Experiencia del Usuario si resuelve primero IPv6

Por ejemplo, un cliente intenta acceder a un servicio *web* en Doble Pila, resuelve por DNS el nombre www.example.com a una dirección IPv4 e IPv6. Si por defecto intenta por IPv6 y la conectividad es muy lenta o inexistente, intentará un número

de veces para después intentarlo por IPv4, que si funciona bien, permitirá acceder a la página *web*. La experiencia del usuario será muy mala y con mucho retardo para cada página que intente cargar, por lo que al final, dejará de verla, como se muestra en la Figura 1.20.

Una solución a este problema es el mecanismo llamado "*Happy-eyeballs*" definido en la RFC 6555. Utilizando el mismo ejemplo de antes y después de resolver la página *web* en las dos direcciones, IPv4 e IPv6, se intenta en paralelo conectar por IPv4 e IPv6, se espera un poco, y si IPv6 no conecta, pero IPv4 si, entonces se decide utilizar IPv4 para acceder a esta *web*. El usuario prácticamente no nota diferencia ya que a él lo que le importa es ver la página *web*, y no el protocolo utilizado para acceder a ella. La información sobre ese dominio se guarda por algún tiempo para evitar hacer el descubrimiento nuevamente, y por lo tanto se evita enviar tráfico innecesario por la red. (Ver Figura 1.21).

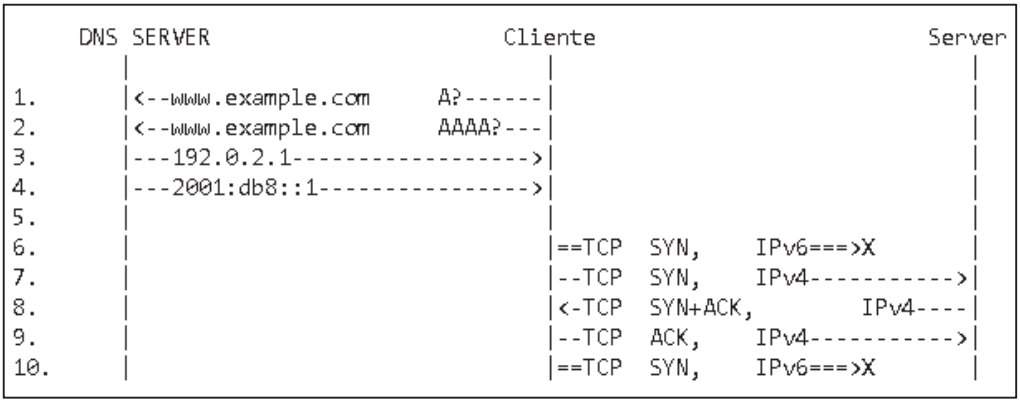


Figura 1.21 Solución *Happy-Eyeballs* [RFC6555]

Esta solución la implementa por defecto el navegador Google Chrome y se puede activar en Firefox, además está presente en el sistema operativo MAC OS y Windows 8.

1.3.7.1.2 Sólo IPv6

Este mecanismo puede hacerse por diversas razones:

- Que no existan suficientes direcciones IPv4.
- Para simplificar la gestión de la red, monitoreo y configuración.
- Para uso en nuevos servicios sólo-IPv6 como las redes de sensores inalámbricos (WSN) basadas en el estándar 6Lowpan (RFC 4919).
- Para montar una granja de servidores sólo-IPv6 para publicar los servicios por Doble Pila mediante balanceadores de carga.

Esta opción tiene un inconveniente, debido a que el acceso ha contenido sólo-IPv4 hacia los nodos que están en la red sólo-IPv6, es limitada. Para esto, existen dos opciones actualmente:

1. *DS-Lite* basado en túneles, IPv4 encapsulado en IPv6, que permite ofrecer IPv4 a los usuarios finales.
2. Mecanismos de traducción llamados NAT64/DNS64 y 464XLAT. Esta solución presenta carencias y habrán cosas que no funcionen. A medida que haya más contenido accesible sobre IPv6, el problema disminuirá.

1.3.7.2 Túneles

Los mecanismos de transición basados en túneles se deben usar cuando se quiere enviar un paquete de una versión de IP a través de una red que no soporta esa versión.

Para ello se encapsula el paquete a enviar en un paquete IP de la versión soportada por la red a atravesar.

Los túneles pueden ser:

- Estáticos Vs Automáticos:
    - Estáticos cuando se configura de manera manual los extremos del túnel.

- Automáticos: Cuando establece su configuración o parte de ella automáticamente, sin necesidad de configurarlo explícitamente.

- Punto a Punto Vs. Multipunto.
  - Punto a Punto: Solamente conectan dos puntos de red, de forma que los paquetes que entran por un extremo del túnel, se encapsulan en otro paquete IP que atravesará una red para llegar al otro extremo del túnel donde se desencapsulará y se extraerá el paquete original.
  - Multipunto: Conectan varios puntos de red o interfaces de túnel, de forma que un paquete que entra en el túnel se encapsula y puede ser entregado en uno de varios posible puntos de salida del túnel.

A continuación se estudiarán los mecanismos de transición IPv6 basados en túneles y que son los más utilizados en la práctica.

1. Túnel 6in4
2. Túnel Broker
3. 6to4
4. 6RD
5. *DS-Lite*

1.3.7.2.1 Túnel 6in4

Los túneles 6in4 consisten en encapsular IPv6, que se identifica por el número de protocolo 41, dentro de un paquete IPv4.

Es un túnel punto a punto estático y configurado manualmente. Se puede encapsular IPv6 en IPv4 directamente, se puede utilizar una cabecera GRE (*Genereric Routing Encapsulation* – RFC 2784) para ello.

Como se ve en la Figura 1.22, para atravesar una red sólo-IPv4, se puede configurar un extremo del túnel en un *router*, y el otro extremo en otro *router* que está conectado al Internet IPv6, por lo que podrá ofrecer servicio de conectividad IPv6 a través del túnel, a toda la red conectada al *router* que establece el túnel.

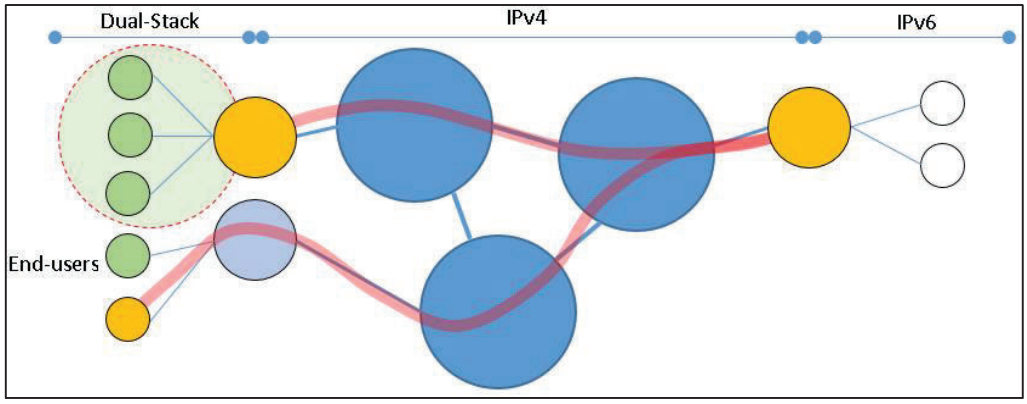


Figura 1.22 Túnel 6in4

También se puede configurar el *router* desde un *host* que de esta manera obtiene conectividad de forma individual.

1.3.7.2.2 Túnel-Broker

El túnel *broker* no es más que un agente que pretende automatizar la creación de túneles 6in4, ofreciéndolos como servicio.

Normalmente, el usuario debe registrarse en una página *web* donde solicita la creación del túnel, y el túnel-*broker* se encarga de configurar su extremo del túnel en el servidor de túneles que suele ser un *router* conectado al Internet IPv6.

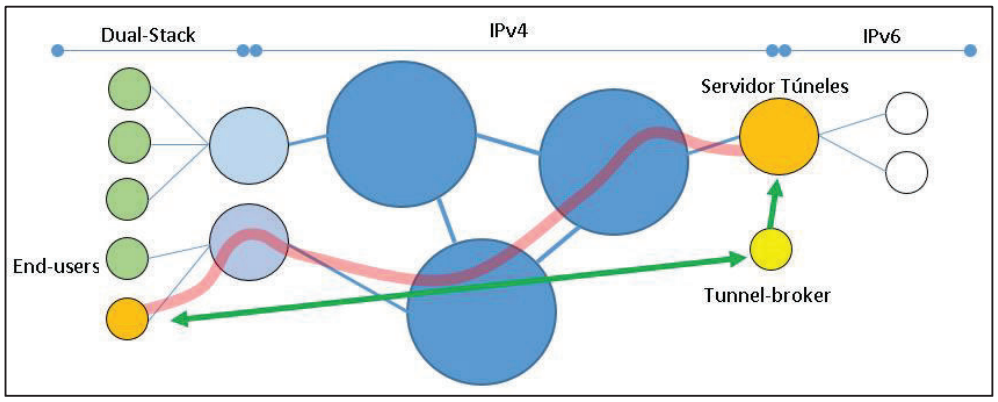


Figura 1.23 Túnel-Broker

El túnel *broker* enviará instrucciones para que el usuario configure su extremo del túnel en función de su IP y el sistema operativo utilizado, entregándole toda la información necesaria para ello.

Una vez configurados ambos extremos, el funcionamiento es similar al que se vio en 6in4. Ver Figura 1.23.

Los siguientes son algunos ejemplos de servicios gratuitos de túnel-*broker* disponibles en Internet y que utilizan distintos protocolos para establecer el túnel punto a punto.

- Freenet6: www.gogo6.com/freenet6/tunnelbroker (*TSP - Tunnel Setup Protocol*).
- HE: tunnelbroker.net (6in4)
- SixXS: www.sixxs.net (6in4, TSP, AYIYA - *Anything In Anything*)

1.3.7.2.3 Túnel 6to4

Los túneles 6to4 se basan en encapsular IPv6 en IPv4, son túneles automáticos y multipunto y además utilizan un prefijo reservado (2002::/16) para este mecanismo de transición. Necesita además una dirección IPv4 pública.

El prefijo 6to4 se construye concatenando el prefijo reservado + los 32 bits de la dirección IPv4 pública, obteniendo un prefijo /48. Este mecanismo de transición creará una interfaz 6to4 virtual que encapsulará/desencapsulará los paquetes IPv6 dentro de IPv4.

El *Relay* 6to4 será un *router* 6to4 y que además conecta al Internet IPv4 con el Internet IPv6. Habrá dos tipos de comunicaciones

- *Host* 6to4 – *Host* 6to4
- *Host* 6to4 – *Host* IPv6 Nativo

Los túneles 6to4 son importante por 2 razones:

1. Por estar siempre disponibles, ya que se activan automáticamente en los sistemas operativos Windows cuando tienen configurada una IP pública en ellos.

2. Por haber sido el origen del mecanismo 6RD que es un mecanismo muy útil y utilizado en la práctica por diferentes LIRs.

1.3.7.2.4 Túnel 6RD

Los túneles 6RD se basan en encapsular IPv6 en IPv4, son túneles automáticos y multipunto. Este mecanismo es una evolución del túnel 6to4 ya que incluye mejoras como las siguientes:

1. No necesita un prefijo reservado, ya que utiliza *Global Unicast Addresses* (GUA) propias del ISP.

2. Puede utilizar direcciones IPv4 privadas, siempre y cuando, en el ámbito donde se utilice el mecanismo 6RD, esas direcciones, sean únicas.

3. Sigue utilizando un prefijo IPv6 concatenando una dirección IPv4 para formar lo que se llama el prefijo 6RD del usuario.

Es una solución muy buena para ISP dado que el uso de 6RD es transparente al resto de Internet. Se utiliza únicamente dentro del ISP donde tiene control de todos los equipos. Habrá dos tipos de comunicaciones:

- Nodo 6RD – Nodo 6RD
- Nodo 6RD – Nodo IPv6 Nativo

Este mecanismo se encuentra disponible en los principales fabricantes y se ha utilizado en la práctica por ISPs.

El prefijo Delegado 6RD es el prefijo 6RD que puede usar el CPE del usuario final para direccionar sus redes internas y está compuesto por el prefijo 6RD, para este mecanismo de transición, usado por el ISP + dirección IPv4 o parte de ella. En

algunos casos se puede eliminar parte de la dirección IPv4, cuando se tienen bits en común en todos los nodos de la red.

Si el prefijo 6RD es menor de 64 bits, el CPE podrá crear subredes de 64 bits. Ver Figura 1.24.

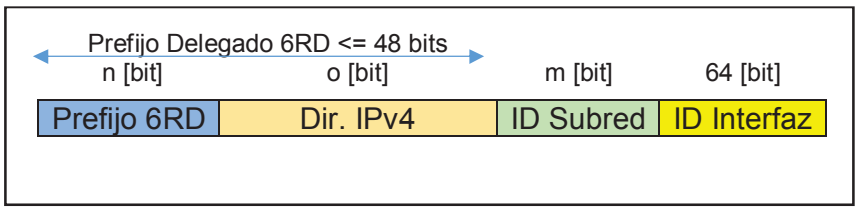


Figura 1.24 Prefijo Delegado 6RD

Por ejemplo, el prefijo 6RD utilizado por el ISP es 2803:0b00::/32, y por lo tanto el bit “n” es igual a 32 bits.

Las direcciones IPv4 utilizadas por todos los CPE y por el ISP internamente pertenecerán al prefijo 10.0.0.0/8, por lo tanto, se tendrán 8 bits que serán comunes a todos los nodos de esa red, es decir, el bit “o” es igual a 24 bits.

De esta forma el prefijo delegado 6RD será un /56 compuesto de los 32 bits del prefijo 6RD + 24 bits de la dirección IPv4.

Si la dirección IPv4 del CPE es la 10.0.0.2, entonces, los 24 bits de menor peso son 0.0.2 y pasándolos a hexadecimal se obtiene :000:02.

De esta manera se puede concatenar el prefijo 6RD+IPv4 y conseguir el prefijo: 2803:0b00:0000:0200::/56. Con este prefijo se pueden crear hasta 256 posibles redes /64.

En la Figura 1.25 se presenta la comunicación entre 2 *host* 6RD entre sí. Se tiene un *router* 6RD que tiene una dirección IPv4 10.0.2.2, pasándolo a hexadecimal se obtiene: 0a00:0202. Se concatena el prefijo 6RD con la dirección IPv4 en hexadecimal y se consigue el prefijo: 2803:0b00:0a00:0202::/64 que se la puede utilizar para asignar a un *host* “A” (2803:0b00:0a00:0202::2/64) que da servicio este *router* 6RD.

De igual manera cualquier otro *router* dentro del ámbito del ISP, con una dirección por ejemplo 10.0.6.6 (:0a00:0606), obtiene el prefijo 6RD y se le asigna a un *host* "B" una IPv6 pública con este nuevo prefijo (2803:0b00:0a00:0606::6/64). A partir de ese momento, los *host* A y B podrían comunicarse entre sí. Para lograr esta comunicación, los paquetes nativos IPv6 viajarían desde la LAN hasta el *Router* 6RD que los encapsularía en IPv4 y lo enviaría hacia el otro *router* 6RD, en donde se desencapsula y lo envía nativo IPv6 al *host* B.

Para el ejemplo de la Figura 1.25, las direcciones utilizadas para el *host* A serían:

- IPv6 origen 2803:0b00:0a00:0202::2/64 (dirección *host* A)
- IPv6 Destino: 2803:0b00:0a00:0606::6/64 (dirección *host* "B")

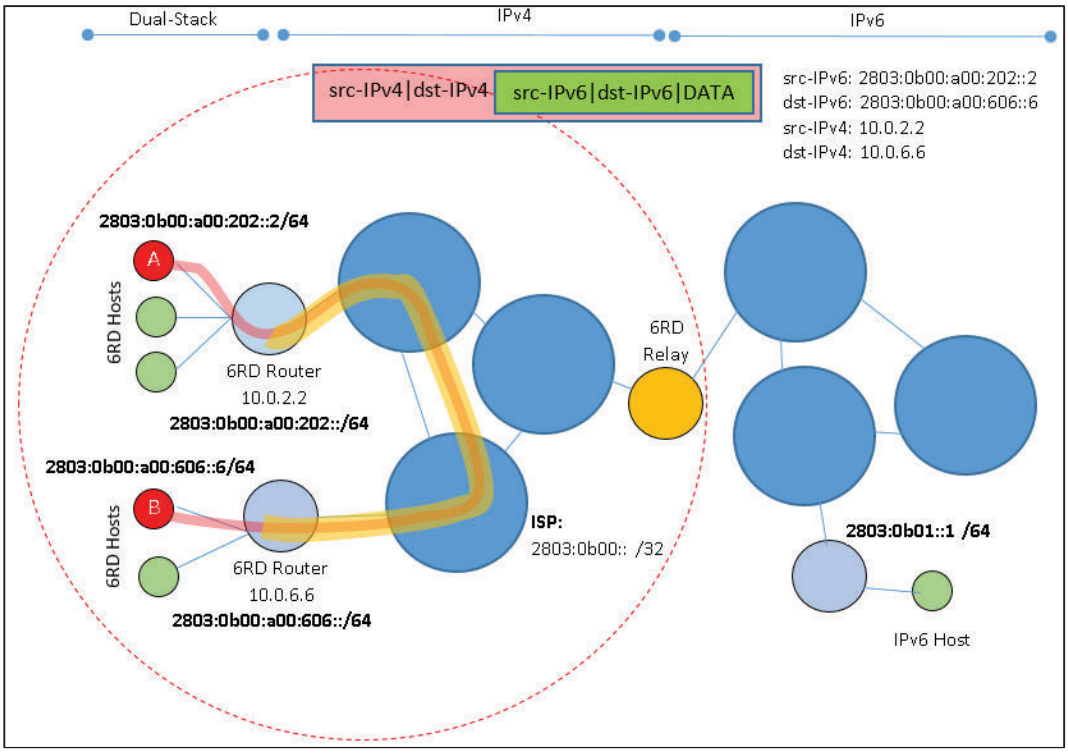


Figura 1.25 Ejemplo de funcionamiento del Túnel 6RD dentro de un mismo ISP

El objetivo en este mecanismo es buscar la dirección IPv4 embebida dentro de la dirección IPv6 destino del *host* "A" ya que al momento que el *router* 6RD ve la dirección destino, sabe que está utilizando el prefijo utilizado para 6RD y por lo tanto puede buscar la dirección IPv4 embebida dentro del prefijo IPv6.

En el caso de querer comunicar 2 *host*, uno “A” que sería un *host* 6RD dentro del ISP y otro “B” que es un *host* en el Internet global – con una dirección global, se requiere un elemento llamado *Relay* 6RD que conecta ambos mundos.

El *Relay* 6RD anunciará hacia la red interna una dirección *anycast* conocida, que se va a utilizar por defecto para enviar tráfico 6RD; y hacia el Internet IPv6 anunciará el prefijo utilizado por el ISP para servicio 6RD. De forma que el *host* “A” enviará los paquetes IPv6 a través del *router* 6RD, que los encapsulará y los enviará sobre IPv4 a través de la infraestructura que es sólo IPv4 hasta el *Relay*. Aquí se desencapsula y se enviará por IPv6 nativo hacia el *Host* “B”, tal como se muestra en la Figura 1.26.

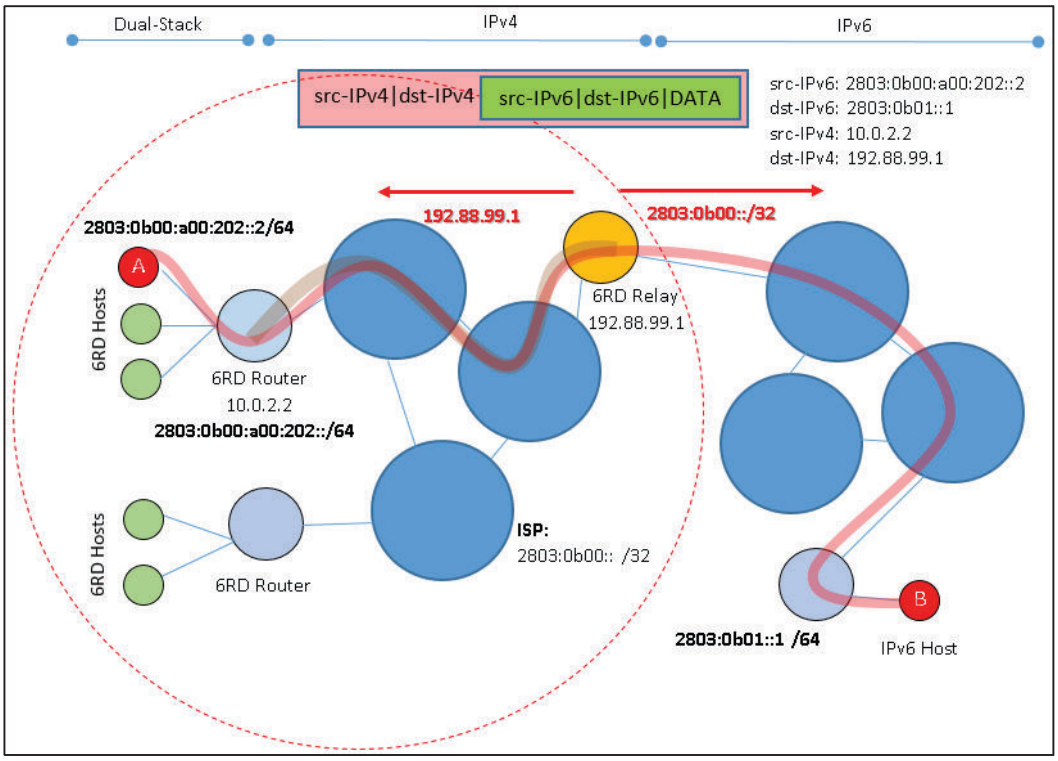


Figura 1.26 Ejemplo de funcionamiento del Túnel 6RD con un host fuera del ISP

El tráfico irá nativo hasta llegar al *router* 6RD, donde se encapsula en un paquete IPv4. La dirección origen IPv6 será la del *host* “A”, la dirección destino será la dirección global del *host* “B”. El *Router* 6RD, al ver que la dirección destino no pertenece al prefijo utilizado por 6RD, sino a una dirección global, encapsulará en

IPv4 utilizando como dirección origen su propia dirección, y como dirección destino, la dirección *anycast* conocida para este servicio 6RD dentro de la red del operador (192.88.99.1).

1.3.7.2.5 Túnel DS-Lite

El túnel *DS-Lite* es un mecanismo de transición avanzado ya que se basa en tener la red principal sólo con IPv6 nativo y encapsula IPv4 dentro de IPv6 para ofrecer conectividad IPv4.

Se ha diseñado para que ayude con el agotamiento de direcciones IPv4 y lo realiza mediante un “NAT Grande” y “Potente” donde se comparten las direcciones IPv4 públicas entre los usuarios. El objetivo de este mecanismo es que sólo se hace NAT una vez en el “NAT Grande” y no en el CPE.

Los elementos del *DS-Lite* se llaman AFTR (*Address Family Transition Router*), también llamado CGN (*Carrier Grade Nat*) o LSN (*Large Scale NAT*). El Cliente que crea el túnel es llamado “B4” (*Basic Bridging BroadBand*).

En la Figura 1.27 se muestra que el tráfico IPv6 se enviará de forma nativa directamente sobre el Internet IPv6. El tráfico IPv4 que llega al CPE “B4” para ser enviado al Internet IPv4, se encapsula en IPv6 en el CPE directamente, sin hacerle nada, y una vez en el AFTR central, se desencapsula y se le hace NAT para enviarlo al Internet IPv4.

Con este mecanismo de transición, el tráfico IPv6 nativo circula nativamente sobre la red IPv6, mientras que el tráfico IPv4 se enviará hasta el CPE “B4” con dirección origen, según la Figura 1.27, la 10.0.02 y dirección destino una dirección global de Internet 1.2.3.4, de forma de que cuando llega al “B4”, se encapsulará en un paquete IPv6 con dirección IPv6 origen la del “B4” y dirección destino IPv6 la del AFTR. Este paquete atravesará la red principal IPv6 y cuando llegue a la AFTR se desencapsula el paquete IPv4, se le aplica NAT, se cambia la dirección origen por una dirección pública que tenga el AFTR (1.1.1.1) y se lo envía al destino (1.2.3.4) el paquete por la red IPv4.

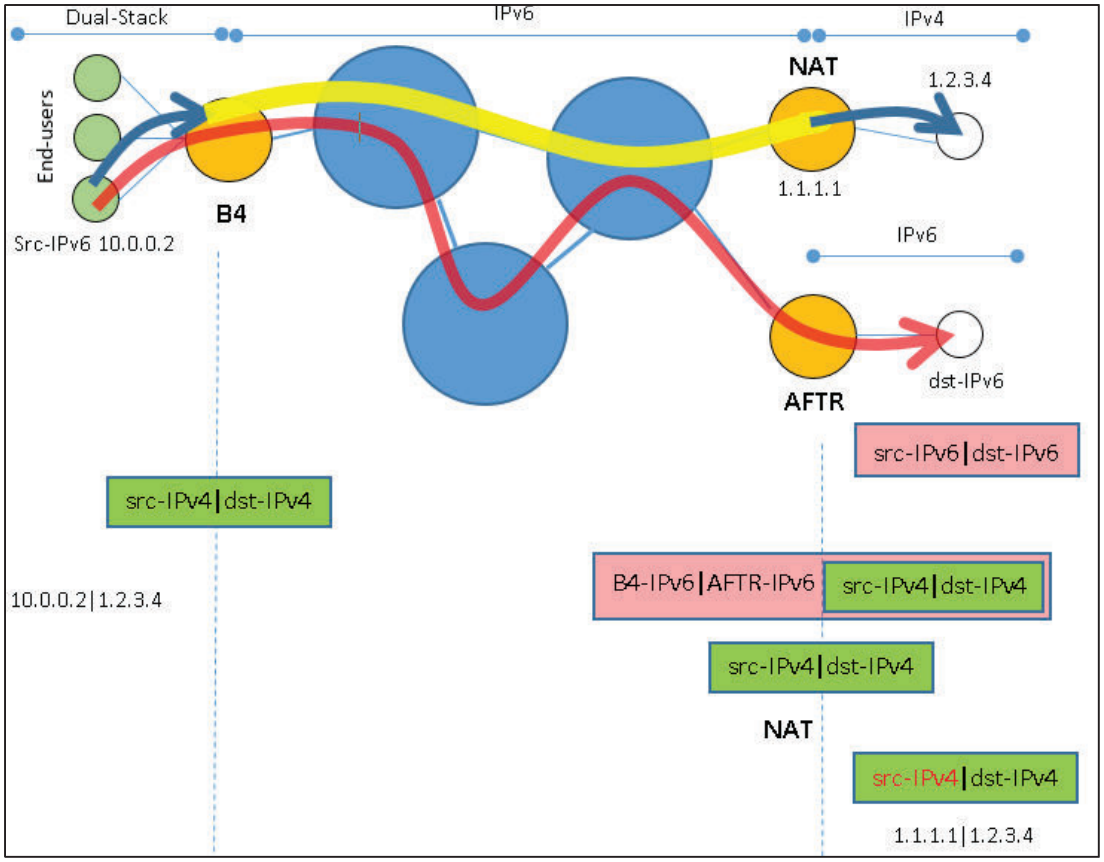


Figura 1.27 Ejemplo del uso del Túnel *DS-Lite*

1.3.7.3 Traducción

Los mecanismos de traducción son los menos recomendados pero son la única opción cuando se quiere comunicar un *host* que sólo entiende una versión del protocolo con otro *host* que sólo entiende la otra versión del protocolo IP.

Para ello hace falta un elemento traductor entre los dos tipos de redes. Según quien inicie la comunicación se tendrá comunicación desde un *host* sólo-IPv6 hacia un *host* sólo-IPv4 o desde un *host* sólo-IPv4 a un *host* sólo-IPv6, esta última opción se considera OBSOLETA (RFC4966) y no se recomienda ya que no existen estándares ni implementaciones para lograr esto.

Si se quiere comunicar un *host* sólo-IPv4 con un *host* sólo-IPv6, se debe ofrecer conectividad IPv6 al *host* sólo-IPv4. Ver Figura 1.28.

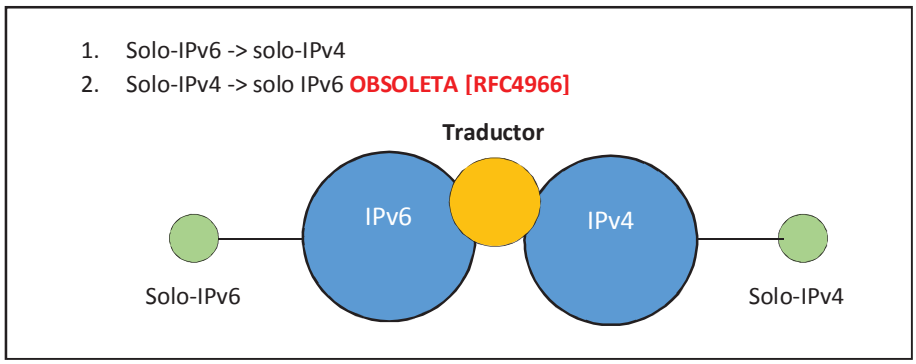


Figura 1.28 Mecanismo de transición basado en Traducción

El contexto donde se puede necesitar la traducción será aquel en el que hayan redes sólo-IPv4 y redes sólo-IPv6. El *host* que inicia la comunicación es el *host* sólo-IPv6 y mediante un elemento llamado traductor, alcanzará el contenido del *host* sólo IPv4

Dentro de los mecanismos de transición basados en traducción se pueden utilizar las siguientes alternativas:

1. NAT64/DNS64
2. 464XLAT

1.3.7.3.1 Mecanismo de transición basado en traducción NAT64/DNS64

El mecanismo NAT64/DNS64 ofrece una solución al escenario donde un *host* sólo-IPv6 desea comunicarse con un *host* sólo-IPv4. Esta traducción está definida únicamente para TCP (*Transmission Control Protocol* – RFC 793), UDP (*User Datagram Protocol* – RFC 768) e ICMP (*Internet Control Message Protocol* – RFC 792). Todo lo que no use esos protocolos, no funcionará.

Los usuarios sólo-IPv6 compartirán direcciones IPv4 públicas, necesarias para comunicarse con el Internet IPv4, por lo que este mecanismo también requiere direccionamiento IPv4 público.

Se basa en la traducción automática de direcciones IPv4 a IPv6 y viceversa, utilizando información estática. Para esto, se utiliza un prefijo conocido (64:ff9b::/96)

al que se le concatena la dirección IPv4. El objetivo es tener una dirección IPv4 útil dentro de la dirección IPv6. Aunque el estándar (IPv6 *Addressing of IPv4/IPv6 Translators* – RFC 6052) define cómo generar estas direcciones automáticamente, la más común es utilizar un prefijo /96 y añadirle los 32 bits de la dirección IPv4, según se muestra en la Figura 1.29.

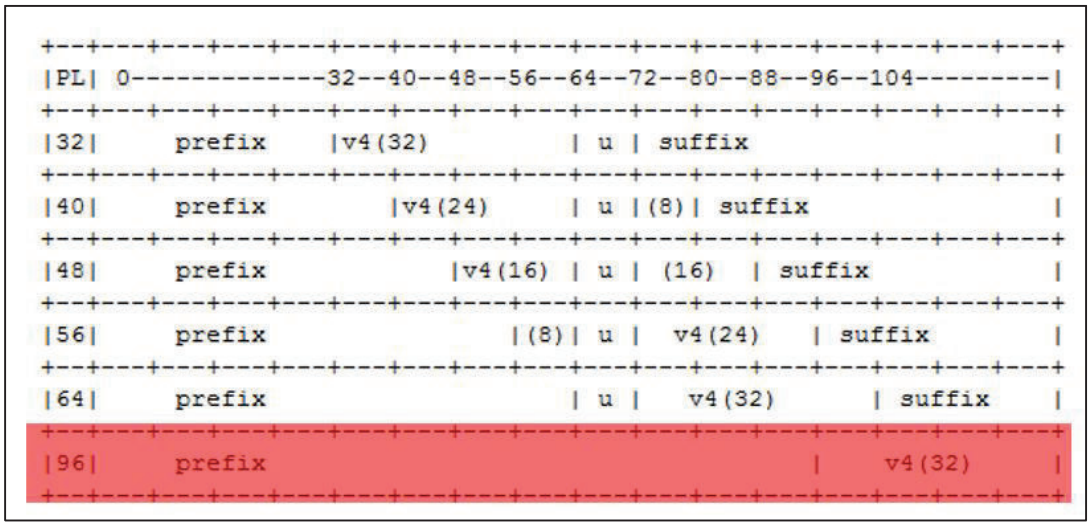


Figura 1.29 Prefijo comúnmente utilizado para NAT64/DNS64 según RFC 6052

Para que este mecanismo funcione, es necesario "engañar" a los nodos sólo-IPv6 para que crean que los nodos sólo-IPv4 son alcanzables mediante una dirección IPv6. Para realizar esto, se define el DNS64 que crea respuestas DNS falsas, devolviendo una dirección IPv6 creada automáticamente a partir de la dirección IPv4 del nodo sólo-IPv6.

NAT64 se puede utilizar en dos escenarios:

1. Conocido como Stateful NAT64: permite a una red sólo-IPv6 acceder a nodos sólo-IPv4, usándose de forma conjunta con DNS64

2. Conocido como *Stateless* NAT64 (sin DNS64): permite mediante una traducción 1 a 1 acceder a todo el Internet IPv6 a un nodo sólo-IPv4

El funcionamiento de NAT64 se mostrará con ayuda de las Figuras 1.30 (*Stateful NAT64*) y Figura 1.31 (*Stateless NAT64*).

Para el ejemplo de la Figura 1.30, se supone que se tiene un *host* sólo-IPv6 que quiere acceder a una *web* sólo-IPv4 (www.example.com). Lo primero que tiene que hacer es consultar a su servidor DNS [1]. En este caso será un DNS64 y hará la resolución en su sistema DNS normal de Internet preguntando por el nombre de dominio www.example.com [2]. En este caso obtendrá como respuesta una dirección IPv4, ya que esa *web* solo está disponible en esa versión del protocolo [3].

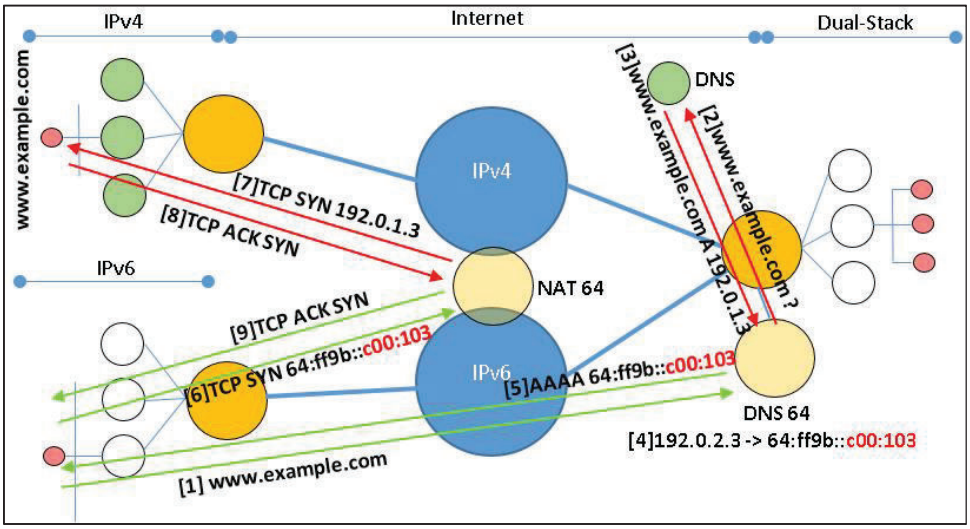


Figura 1.30 *Statefull* NAT64/DNS64

El DNS64 generará automáticamente una dirección IPv6 concatenando un prefijo IPv6 a la dirección IPv4 recibida por DNS [4], de forma que responde a la petición DNS con una dirección IPv6 [5], y el *host* pensará que esa *web* está disponible sobre IPv6.

El *host* tratará de establecer la conexión TCP [6] dirigida a esa dirección IPv6 generada de manera automática. Todo el tráfico con dirección al prefijo /96 que se está usando para la solución NAT64, acabará por *routing* interno en los *routers* que hacen el NAT64 [7] y que traducirán el tráfico IPv6 a tráfico IPv4.

La dirección destino de los paquetes IPv4 va embebida dentro de la dirección destino IPv6 (192.0.1.3). De esta forma, el tráfico llegará al servidor y responderá

como si le preguntaran desde IPv4 [8], pero al *router* NAT64 que deshacerá la traducción y lo enviará al *host* A [9].

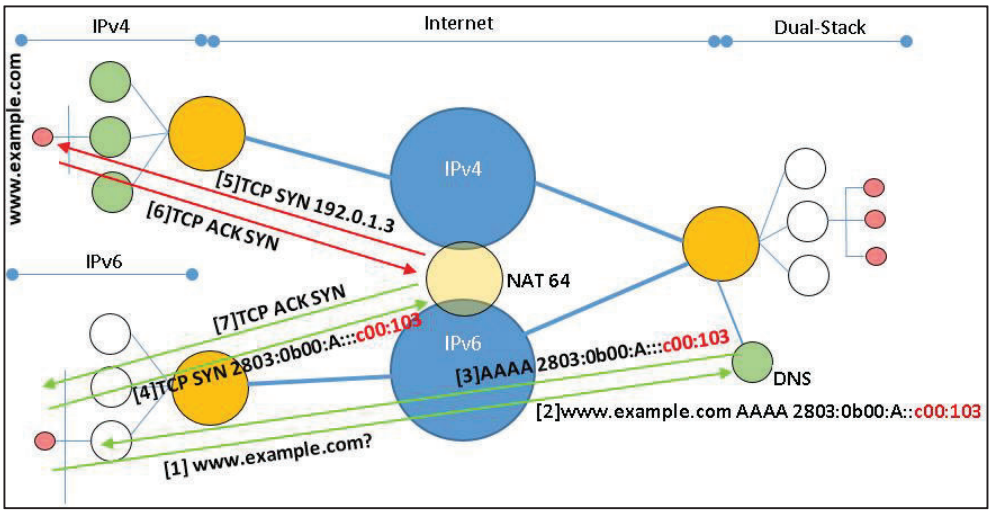


Figura 1.31 *Stateless* NAT64/DNS64

En el escenario *Stateless* NAT64, mostrado en la Figura 1.31, ya no existe el DNS64, aquí el servidor que publica la *web*, añadirá una entrada en el DNS normal con una dirección IPv6 global que le pertenece y que además lleva embebida la dirección IPv4 del servidor *web*. De esta manera, cuando el *host* alcanza el *router* NAT64 [1], éste puede traducir automáticamente [2] utilizando como dirección destino IPv4 que va dentro de IPv6 [3].

El resto del proceso se lo realiza de la misma manera que el caso *Statefull* NAT64. Pasos [4], [5], [6] y [7].

Un ejemplo común de uso sería un balanceador de carga que redistribuya peticiones IPv6 a una granja de servidores sólo IPv4.

Se debe recordar que NAT 64 es un mecanismo de traducción, que es la última opción a considerar ya que presenta limitaciones y problemas como los siguientes:

- Está definido únicamente para tráfico *unicast* TCP, UDP e ICMP.

- Existirán aplicaciones que utilizan información de capa 3 (capa de Red) en la capa de Aplicación, como FTP o SIP/H323, en donde se requerirá de un ALG (*Application Layer Gateway* – RFC 6384) para que realice modificaciones en la capa de Aplicación de los paquetes.

- Se requerirán nuevos *routers* que funcionen como NAT64 y como DNS64.

- Funciona bien con nombres de dominio DNS pero, ¿qué pasaría si una aplicación trata de usar una dirección IP?, entonces no funcionaría, ya que el DNS64 no será capaz de realizar la traducción automática de las direcciones.

- Las aplicaciones que no soportan IPv6 tampoco funcionarían.

1.3.7.3.2 Mecanismo de transición basado en traducción 464XLAT

464XLAT resuelve los problemas vistos por NAT64 y es una combinación de un *Statefull* NAT64 (*Core*) + *Stateless* NAT64 (Borde), es decir, se hace traducción dos veces. Está definido en la RFC 6877.

Esta solución funciona en el modelo Cliente – Servidor, cuando el servidor tiene una dirección IPv4 global. Se definen dos traductores:

1. CLAT (*Customer-Side-Translator*): Traduce algorítmicamente uno a uno una dirección IPv4 privada a una dirección IPv6 global y viceversa.

2. PLAT (*Provider-Side-Translator*): Realiza una traducción N a 1 de direcciones IPv6 globales a direcciones IPv4 públicas y viceversa.

El funcionamiento de este mecanismo se presenta en un escenario típico, una red de telefonía móvil, mostrado en la Figura 1.32.

En este caso, el CLAT se encontraría dentro del propio terminal de usuario y el PLAT a la salida de la red del operador hacia el Internet IPv4.

El tráfico IPv6 circularía sin problema y de forma nativa por la red, en cambio, una aplicación que solo soporte IPv4 con una dirección IPv4 privada, generaría tráfico

IPv4 y el CLAT lo traduciría a tráfico IPv6. Ese tráfico atravesaría la red del operador hasta llegar al PLAT, en donde se volvería a traducir a tráfico IPv4 utilizando direcciones globales.

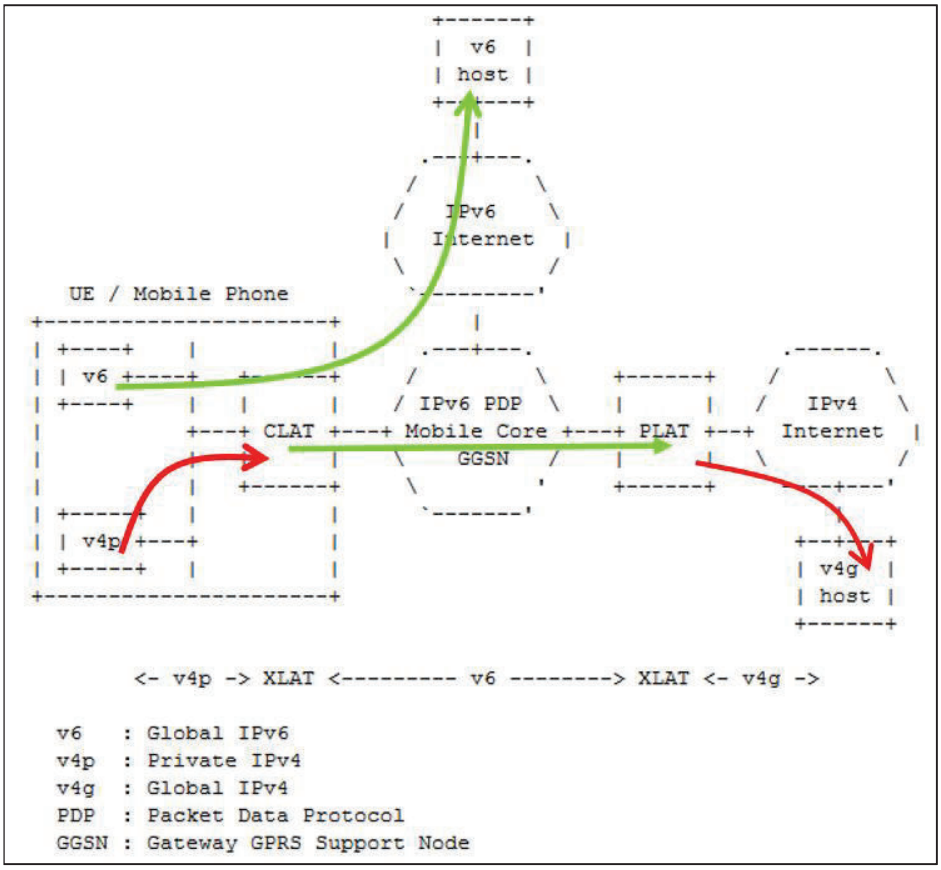


Figura 1.32 Uso del mecanismo 464XLAT en una red de telefonía Móvil

1.4 RECOMENDACIONES GENERALES

Se darán recomendaciones generales sobre el agotamiento de direcciones IPv4, sobre el aumento de IPv6 y sobre la planificación de la transición y su coexistencia.

1.4.1 AGOTAMIENTO DE DIRECCIONES IPv4

El agotamiento de direcciones IPv4, en todo el mundo, se ha prolongado por el uso de políticas para la asignación de direcciones IPv4. A pesar del anuncio de la IANA

que entregó los últimos /8 a cada RIR en el mundo, todavía existen direcciones IPv4 para los usuarios finales.

En el caso de LACNIC, en donde existen 4 fases de agotamiento de direcciones IPv4, se ha determinado que actualmente está en la fase 2, en la cual se asignan como máximo bloques /22 que equivale a 1024 direccione IP, quien recibe esos recursos, solo puede solicitar un bloque adicional a los 6 meses.

En la fase 3 (final), se asignarán únicamente bloques, máximo /22, a nuevos miembros.

Según las ultimas noticias de LACNIC, la devolución de bloques IPv4, cambió la perspectiva de agotamiento, y hay más direcciones disponibles para la fase 3 (6.626.098 direcciones IPv4), con esta cantidad se estima que quedan direcciones IPv4 hasta el 2024.

Por eso se propuso una nueva política para modificar el alcance de la fase 2 y se propone distribuir los 2 bloques, de la fase 2 y la fase 3, de forma que cada fase tenga una cantidad más equitativa de direcciones IPv4. Esta política amplia la duración de la fase 2, y mantiene el criterio de asignación empleado hasta ahora.

1.4.2 EL AUMENTO DE IPv6

El aumento de IPv6 es un hecho hoy en día, está aumentando el tráfico, el soporte en productos, hardware y software, formación de ingenieros, etc.

El tráfico IPv6 está creciendo de manera exponencial, al 12 de noviembre 2015, ha alcanzado el 7.33% del tráfico de Internet [12], aunque algunos países o regiones superan ampliamente esta cifra.

Existen cada vez más redes sólo-IPv6, o que están considerando implementar solamente IPv6, y tratando de usar mecanismos de transición para ofrecer conectividad a contenidos IPv4. Los mecanismos, como se ha visto, tienen limitaciones, por lo tanto, si no se desea volver invisible o borroso a una parte creciente de Internet, se deberá ser alcanzable por IPv6.

Además están desarrollando nuevas tecnologías como los sensores inalámbricos (*Wireless Sensor Networks*) que se basan en protocolos definidos solamente para IPv6, como es *6lowpan*. Está claro que el futuro pasa por IPv6 y se debe estar preparado para ello.

1.4.3 PLAN DE TRANSICIÓN Y COEXISTENCIA

La transición a IPv6 y la coexistencia con IPv4 deben planearse adecuadamente, ajustando el proceso a cada caso en concreto. Cada organización debe hacerse cargo de su infraestructura a implementar IPv6, como si se tratara de otro proyecto de innovación tecnológica. Este proyecto será más o menos complejo dependiendo de cada caso, tamaño de red, componentes, procesos internos, presupuesto, etc.

Los puntos a tener en cuenta al momento de llevar a cabo este proyecto son:

- Estudio de viabilidad. ¿Es posible o no es posible? Se puede decir que si, ya que de una manera u otra, se logrará ofrecer conectividad IPv6 a la red IPv4 utilizando una de las múltiples herramientas como los mecanismos de transición estudiados.

- ¿El porqué? El primer paso es encontrar una razón para llevarla a cabo, ya sea por recomendaciones, mandatos legales de gobierno, por estar a la vanguardia tecnológica, para buscar nuevas oportunidades de negocio. Hoy en día la duda no es si hacerlo o no, la duda es cuándo hacerlo, y mientras más pronto, mejor.

- ¿Quién? Hay que ver que departamentos, organismos o personas participarán y se verán involucrados en este proyecto.

- ¿Cómo? Consistirá en identificar y programar tareas y fases, nombrar un coordinador, etc.

- ¿Cuándo? Se deben establecer plazos, ya que cada vez más se está volviendo más urgente implementar IPv6.

Como en todo proyecto, hay que fijar un objetivo final, un alcance del mismo para saber cuándo se ha cumplido y por lo tanto cerrar el proyecto.

Existen otros aspectos más concretos a tener en cuenta y que se deben abordar en la transición a IPv6:

- Formación del personal involucrado: este paso se lo debe llevar a cabo al principio ya que permitirá un adecuado desarrollo del proyecto.
- Analizar la red existente, teniendo en cuenta los cambios a corto plazo y evaluando la topología, los servicios, tecnologías, etc.
- Inventariado completo de los elementos que componen la red. En función de esto, se establecerán las funcionalidades IPv6 necesarias para implementar IPv6 y cuáles de estas funcionalidades son soportadas por los elementos que se han inventariado.
- Se debe llevar a cabo un plan de direccionamiento desde un prefijo IPv6 que se lo deberá solicitar al RIR correspondiente.
- La conectividad IPv6 se la debe evaluar, buscando proveedores e intentando conseguir una conectividad nativa.
- Se debe abordar una estimación de costos, tanto de elementos de la red, así como también, de gestión y control de la nueva red.
- Se debe decidir una estrategia, decidir cómo se lo va a realizar y si se va a implementar IPv6 solo, en Doble Pila u otros mecanismos de transición. Definir en qué partes de la red se realizará cada uno de los mecanismos de transición.
- Implementación de un plan piloto para realizar pruebas transparentes al usuario, antes de poner la nueva red en producción.
- Debe verse a IPv6 como el primer paso hacia la red del futuro, ya que se pueden ofrecer nuevos servicios y tecnologías que utilicen IPv6.

- Todo este proceso es una oportunidad para tratar de mejorar la red, servicios y gestión.

- A largo plazo se puede pensar en eliminar IPv4, de forma que se implemente, parte de la red o la red completa y servicios, solo con IPv6.
- La primera opción en la estrategia debe ser Doble Pila.

- Cuando Doble Pila no sea posible y se tenga una infraestructura IPv4, se pueden utilizar soluciones como:

    - 6in4: solución simple, muy útil a veces y se la puede utilizar para realizar pruebas. No es escalable ya que es un mecanismo que conecta punto a punto y se debe configurar manualmente.

    - *Túnel-Broker*: solución para pruebas, para tener conectividad en una pequeña red.

    - 6RD: solución escalable y fácil de implementar siempre que se tenga un buen soporte en el CPE. Para un ISP es una buena solución temporal.

- Si ya se tiene una infraestructura IPv6, se pueden utilizar soluciones como:

    - *DS-Lite*: solución disponible y escalable ya que crea túneles multipunto de manera automática, optimiza el uso de direcciones IPv4 públicas, siempre y cuando se tenga un buen soporte en los equipos CPE de los clientes.

    - NAT64/DNS64 y su mejora con 464XLAT

1.5 ENRUTAMIENTO IPv4 E IPv6

Una vez analizados los protocolos IPv4 e IPv6 se verá brevemente los protocolos de enrutamiento IPv4 y con más detalle los protocolos IPv6.

En cada uno de los protocolos se estudiarán enrutamiento estático, enrutamiento dinámico IGP y enrutamiento dinámico EGP.

1.5.1 FUNCIONAMIENTO DE LOS *ROUTERS*

Como ya se conoce, los *routers* tienen dos funciones básicas:

1. Enrutamiento: relacionado con la información que se intercambian entre sí los *routers* en el plano de control o que obtienen localmente. El resultado son las tablas de rutas que indican hacia donde enviar los paquetes, normalmente en función de la dirección destino.

2. Reenvío (*Forwarding*): consiste en transferir paquetes entre interfaces utilizando la tabla de reenvío que se alimenta de las tablas de enrutamiento, es decir, la tabla de reenvío consiste en la mejor información seleccionada de las distintas tablas de rutas que hay en el *router*. El reenvío se lleva a cabo normalmente según la dirección destino del paquete IP y se utiliza la ruta más específica (*Longest Prefix Match*).

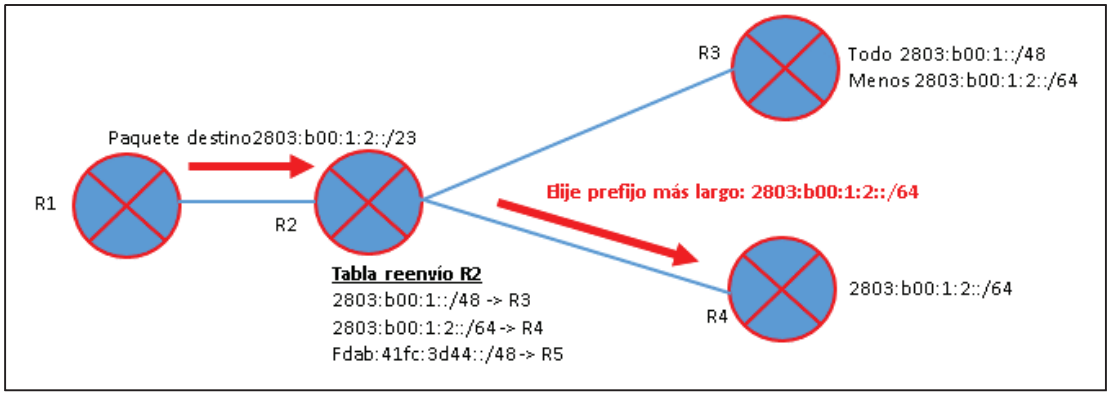


Figura 1.33 Ejemplo de reenvío en *Routing* IPv6

En la Figura 1.33, se presenta un *router* 2 (R2) que tiene una tabla de reenvío con 3 entradas, apuntando el prefijo 2803.b00:1::/48 hacia R3, el prefijo 2803:b00:1:2::/64 al *router* R4 y el prefijo fadb:41fc:3d44::/48 al *router* R5. Si R2 recibe un paquete con dirección destino 2803:b00:1:2::1/23, mirará en su tabla de

reenvío y encontrará tanto la primera ruta como la segunda ruta. La tercera ruta no valdría para llevar este paquete.

De las dos rutas válidas, es decir la que dentro del prefijo va incluida la ruta del paquete, la más específica sería la que apunta al *router* 4, es decir, la más larga, la que tiene más bits coincidentes.

1.5.2 INFORMACIÓN DE ENRUTAMIENTO

La información de enrutamiento se conoce que puede ser:

- De origen estático o manual
- Aprendida por tratarse de interfaces conectadas al *router*
- Aprendida mediante protocolos de *routing* dinámicos

Normalmente en el *router* coexisten varias de estas fuentes de información. A diferencia de los *routers* con Doble Pila, donde hay IPv4 e IPv6 a la vez, la información de enrutamiento IPv4 e IPv6 se gestiona de forma independiente y en paralelo.

Otro concepto usado en *routing* es la distancia administrativa que es usado para desempatar cuando hay dos rutas hacia el mismo prefijo obtenidas de fuentes distintas, por ejemplo, se puede dar más preferencia a las rutas estáticas sobre las que se aprenden por un protocolo de *routing* dinámico como OSPF.

Esta distancia administrativa se usará tanto para desempatar entre rutas IPv4, o entre rutas IPv6, no entre IPv4 e IPv6. La distancia administrativa tiene un significado local en ese *router* solamente.

En la Figura 1.34, se muestra el funcionamiento de los protocolos de *routing* (básicamente). Se dispone de un *router* R1 que da servicio a la Red 1, y otro *router* R2 que da servicio a la Red 2.

Los dos *routers* inicialmente solo conocerán las rutas para llegar a cada una de sus redes. Si decidimos conectarlos entre sí, con un enlace, ambos *routers* aprenderán

también cómo llegar a la Red 3, que será la utilizada entre el enlace entre ambos. Lo que se requiere es que la Red 1 y la Red 2 se comuniquen entre sí, para lo cual son necesarios tres elementos.

1. Información sobre redes/prefijos que se deben enviar y recibir para crear las tablas de ruta.
2. *Next Hop* o dirección donde se puede alcanzar esa red/prefijo.
3. Comunicación entre vecinos (*routers* que están directamente conectados entre sí).

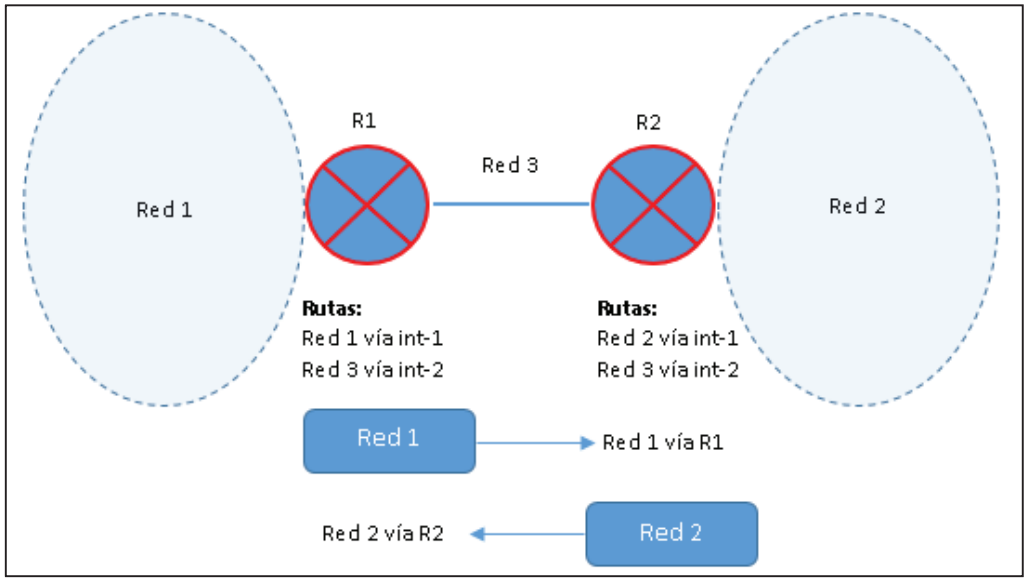


Figura 1.34 Funcionamiento de los protocolos de *Routing* básico

Continuando con el ejemplo de la Figura 1.34, el *router* 2 enviará la información sobre la red 1, con el *Next Hop* donde estará la dirección IP del *router* 1 y en la interfaz que tiene conectada hacia el *router* 2. Este envío se hace sobre IP, de esta forma, R2 aprende dónde enviar los paquetes dirigidos a la Red 1.

De igual manera hace el *router* 2 enviando la información sobre la Red 2 al *router* 1. A partir de ese momento, los *host* en la Red 1 y en la Red 2 se pueden comunicar entre sí.

Los tres elementos vistos se usan tanto con IPv4 como con IPv6, de forma que en general, para añadir IPv6 a un protocolo de *routing* dinámico, habrá que añadir la capacidad para soportar IPv6 en esos tres elementos.

Normalmente IPv4 e IPv6 se usan de manera independiente y en paralelo en un entorno de Doble Pila.

1.5.3 *ROUTING* ID

Los protocolos de *routing* dinámicos requieren un "*router* ID" o identificador de *router* para que se identifique de forma única cada uno de los participantes en el protocolo de *routing* dinámico.

Para este propósito se usa un **número entero de 32 bits.**

- En IPv4 se usa el formato IPv4, es decir una notación de 32 bits, a.b.c.d.
- En IPv6 también sirve el formato usado para IPv4 y realmente así se lo usa. Las reglas para definirlo son las mismas que se usan para *routing* dinámico IPv4.
    - Se puede especificar de forma explícita, con un comando asociado al protocolo de *routing "router-id* a.b.c.d"
    - Si no, el *router* buscará de manera automática por las distintas interfaces configuradas la mayor dirección IPv4 configurada en las interfaces de *loopback.*
    - Si no, la mayor dirección IPv4 de cualquier interfaz no *loopback*.

1.5.4 ENRUTAMIENTO ESTÁTICO

Una ruta estática es una ruta introducida manualmente en la tabla de rutas de un *router*. Tanto su creación como su cambio deben hacerse de manera explícita y es una de las múltiples fuentes de información que posee un *router* para elaborar su tabla de reenvío.

Se diferencian de las rutas dinámicas, o creadas por protocolos de *routing*, en que no reaccionan a cambios en la red de forma automática.

Las rutas estáticas tienen como ventajas lo siguiente:

- Simplicidad a la hora de planificar e implementarlas
- Rapidez para implementarlas y que esa ruta sea efectiva.

Las rutas estáticas tienen como inconvenientes lo siguiente:

- No son una solución escalable para una red grande con muchas rutas y *routers*.
- No son una buena solución a los cambios de la red ya que se necesitaría de alguien que cambie las rutas según los cambios que se produzcan en la red.

El uso y sintaxis de rutas estáticas con IPv6 es similar al de IPv4. Por ejemplo como se ve en la Figura 1.35, en Cisco IOS, la sintaxis es la misma que para IPv4, se debe cambiar IP por IPv6 y también se deben usar parámetros IPv6, como el prefijo, longitud, dirección de *next hop*, etc.

```
ipv6 route prefix/lenght {outgoing interface [next-hope-address] |
next-hope-address } [admin-distance]
```

Figura 1.35 Configuración de Rutas estáticas en Cisco IOS

Sin embargo existen algunas diferencias

- Como dirección ***next-hop*** se puede usar cualquiera del *router* vecino, incluida la dirección ***link-local*.**
- **Si se usa la dirección *link-local*** como *next-hop*, hay que configurar tanto la **interfaz de salida** como la dirección de *link-local*, es decir, hay que poner en *next-hop* la dirección *link-local* del vecino y obligatoriamente indicar por cuál interfaz deben salir esos paquetes.

Esto se debe a que todas la interfaces del *router* tienen direcciones *link-local* que pertenecen al mismo prefijo y, por lo tanto, el *router* no tiene manera de saber a cuál interfaz se debe enviar, si no se indica explícitamente.

1.5.5 ENRUTAMIENTO DINÁMICO IGP

Atendiendo al ámbito en el que se usan los protocolos de *routing* dinámico se pueden clasificar como:

- EGP (*Exterior Gateway Protocol*): se utilizan para intercambiar información entre sistemas autónomos AS.
- IGP (*Interior Gateway Protocol*): se utilizan dentro de un sistema autónomo.

Se debe recordar que Internet está formada por AS, o sistemas autónomos, que están identificados cada uno por un número único y gestionado cada uno por una organización. Dentro de cada sistema autónomo puede haber las redes que se consideren necesarias y utilizan los protocolos y políticas que se crean convenientes de manera independiente a los demás sistemas autónomos. (Ver Figura 1.36).

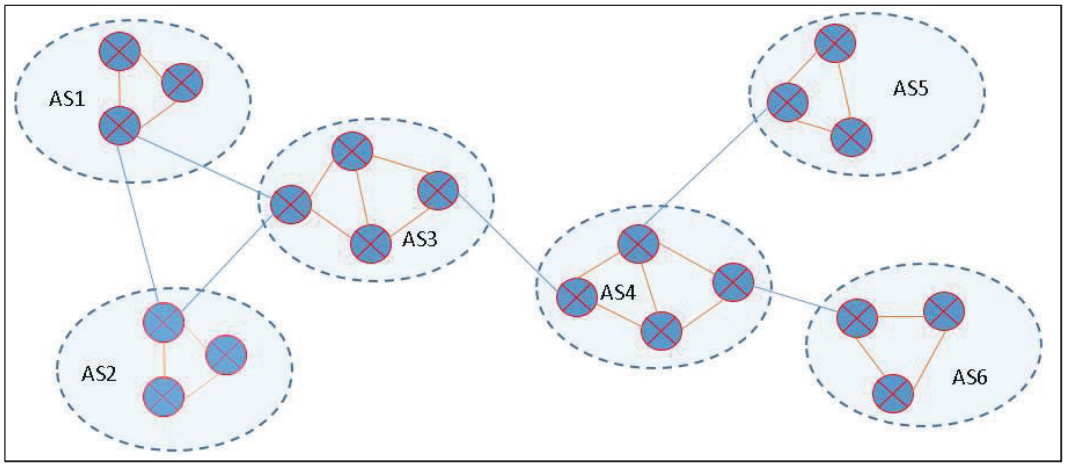


Figura 1.36 EGP vs IGP

1.5.5.1 Protocolos IGP

Atendiendo a la metodología de propagación se pueden clasificar los protocolos IGP en dos tipos:

1. Vector Distancia: utiliza como medida de distancia el número de saltos para llegar a una ruta.
2. Estado de Enlace: se utiliza como medida para calcular la mejor ruta valores asociados a los enlaces, por ejemplo el ancho de banda.

Tabla 1.8 IGP existentes y estandarizados para IPv6

Tipo	Nombre	IPv4	IPv6	Comentarios
IGP	RIP	RIPv2	RIPng	Nueva versión sólo-IPv6
	OSPF	OSPFv2	OSPFv3	Nueva versión sólo-IPv6
	IS-IS	IS-IS	IS-IS	Se extendió para soportar IPv6
	EIGRP	EIGRP	EIGRPv6	Propietario Cisco

Existen varios protocolos IGP, tanto como para IPv4, como para IPv6 y se pueden aplicar distintos criterios de selección, aunque en cualquier caso, para IPv6 se seguirán las mismas directrices que para IPv4.

Los IGP de la Tabla 1.8, son las versiones existentes para IPv6 que están estandarizados.

1.5.5.1.1 Protocolo de enrutamiento RIPng

Rip Next Generation (RIPng – RFC 2080) es una extensión de RIPv2 para soportar IPv6. Lo hace mediante el soporte de direcciones y prefijos de 128 bits (*Next Hop*) y el uso de *multicast* IPv6 para el envío de los mensajes informativos, para ello se reserva la dirección *multicast* IPv6 FF02::9 para todos los *routers* RIP (*all-RIP-routers*). Para tener seguridad en RIPng, se debe usar IPsec con IPv6 ya que no incluye ningún mecanismo de protección específico.

Se puede decir que en general RIPng y RIPv2 son muy parecidos. En la Tabla 1.9 se presentan las semejanzas y diferencias.

A la hora de implementar RIPng en alguna red, se debe tener en cuenta que este protocolo solo sirve para IPv6, de forma que si se dispone de una red Doble Pila, IPv4 e IPv6, se debe implementar RIPv2 para IPv4 y RIPng para IPv6.

Al habilitar RIPng en una interfaz, al igual que en otras versiones de RIP, hará tres cosas:

1. Enviar actualizaciones RIP por esa interfaz.
2. Procesar las actualizaciones RIP recibidas en esa interfaz, por otros procesos que estén corriendo RIP en el mismo enlace.
3. Anunciar las rutas "conectadas" de esa interfaz.

Tabla 1.9 Diferencias y Semejanzas entre RIPv2 vs RIPng

RIPv2	RIPng
DIFERENCIAS	
Mensajes RIP usan UDP sobre IPv4 para envío de mensajes	Mensajes RIP usan UDP sobre IPv6 para envío de mensajes
Puerto UDP:520	Puerto UDP:521
Puede efectuar sumarización automática	No disponible
Dirección *Multicast* usada para updates: 224.0.0.9	Dirección *multicast* usada para updates: ff02::9
Autentificación: específica de RIP	Autentificación: IPv6 AH/ESP
SEMEJANZAS	
Vector Distancia, distancia administrativa por defecto 120, soporta VLSM	
Uso de mecanismos como "*Split horizon*" y "*poison reverse*" para evitar bucles	
Misma métrica: cuenta de saltos, 16 saltos significan infinito	
Actualizaciones completas periódicamente cada 30 segundos (ligeramente variable), sirve para saber que el vecino sigue "vivo"	

RIPng usará direcciones *link-local* como *next-hop*

1.5.5.1.2 Protocolo de enrutamiento OSPFv3

Para soportar IPv6 se definió OSPFv3 [RFC 5340] que modifica OSPFv2 para soportar:

- Direcciones usadas como *Next-Hop* y prefijos de 128 bits mediante nuevos *Link State Advertisement* (LSA – RFC 2370).
- Uso de direcciones *multicast* IPv6 para comunicarse.
    - FF02::5 Para todos los *routers* OSPF (*all-SPF-routers*).
    - FF02::6 Para todos los *Designated routers.*
- Se puede ofrecer IPsec para ofrecer autenticación, algo que OSPFv2 no soporta.
- Hay mensajes independientes de la versión IP, incluidos los LSA.
- Funciona sobre un enlace y no sobre una red IP como OSPFv2.

En general OSPFv2 y OSPFv3 son muy parecidos, en la Tabla 1.10 se presentan las semejanzas y las diferencias de cada uno.

Tabla 1.10 Diferencias y Semejanzas entre OSPFv2 vs OSPFv3

OSFPv2	OSPFv3
DIFERENCIAS	
Mensajes OSPFv2 usan IPv4 para el envío de sus mensajes	Mensajes OSPFv3 usan IPv6 para el envío de sus mensajes
Comprobaciones para estableces los “vecinos”	Iguales, menos: no necesario en la misma subred
No permite varias instancias de OSPF por interfaz	Sí permite varias instancias de OSPF por interfaz
Direcciones *Multicast* usadas: 224.0.0.5, 224.0.0.6	Direcciones *Multicast* usadas: FF02::5, FF02::6
Autentificación: específica de OSPF	Autentificación: IPv6 AH/ESP
SEMEJANZAS	
Estado de enlace, métrica basada en AB interfaz, Protocolo IP: 89, soporta VLSM	
Mismos mecanismos: *flooding*, elección *Designated Router*, soporte de áreas, cálculo SFP de la ruta más corta	
Mismo mecanismo elección *Router* ID, mismos *Hello*, DD o DBD, LSR, LSU y LSAck	
Capacidades opcionales, incluidos: *demand circuit y Not-So-Stubby Areas* (NSSAs)	

OPFv3 [RFC 5340] se definió inicialmente solo para IPv6, de forma que si se tenía una red Doble Pila, con IPv4 e IPv6, se debía implementar OSPFv2 para IPv4 y

OSPFv3 para IPv6, eran dos procesos distintos, cada uno con su configuración propia, tabla de rutas, etc.

OSPFv3 [RFC 5838] se modificó posteriormente para soportar varias familias de direcciones o *Address Family* (AF). OSPFv3 puede tener varias instancias o procesos corriendo a la vez, lo que se puede aprovechar para asociar un *address family* distinta a cada instancia. Esto se hace utilizando el campo *Instance-ID* en la cabecera del paquete OSPFv3. De esta forma se puede tener una instancia OSPFv3 para IPv4 y otra para IPv6.

OSPFv3 usará direcciones *Link-Local* como *Next-Hop* y un *Router-ID* de 32 bits.

1.5.5.1.3 Protocolo de enrutamiento IS-IS

IS-IS es un protocolo de encaminamiento OSI diseñado para soportar el protocolo CLNP (*Connection Less Network Protocol*) [13], que es un protocolo de la capa de Red, similar a IP.

IS-IS corre directamente sobre la capa Enlace, por lo que es independiente de la capa 3 utilizada. Esto facilitó el trabajo de extender su soporte a otros protocolos de Red como IPv4 e IPv6 [RFC 5308].

Es un protocolo de Estado de Enlace que calcula la mejor ruta mediante el algoritmo SPF (*Shorted Path First*) [14].

Permite dividir la red en distintas áreas, estableciendo dos niveles jerárquicos, *Level* 1 y *Level* 2. (Ver Figura 1.37).

La información de *routing* en IS-IS se envía en campos con formato TLV (*Tag / Length / Value*) de forma que para soportar IPv6 se definieron 2 nuevos TLV:

1. IPv6 *Reachability* -> Incluye información de un prefijo IPv6
2. IPv6 *Interface Address*-> Incluye información de un *Next-Hop* IPv6

Se define un nuevo identificador de protocolo IPv6, IPv6 NLPID (*Network Layer Protocol ID),* para indicar que se está usando IPv6 con IS-IS.

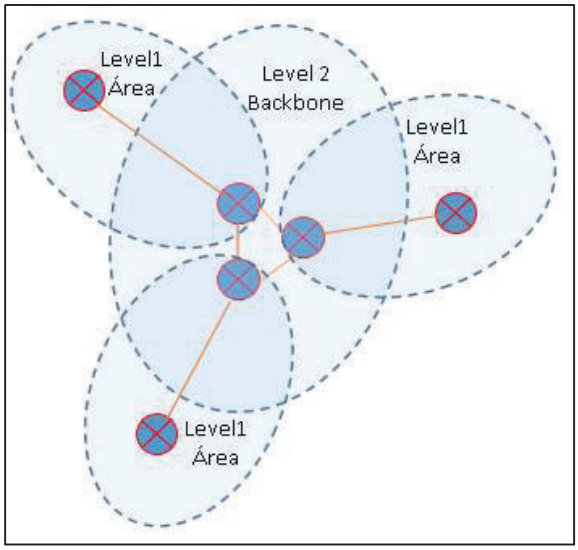


Figura 1.37 Protocolo IS-IS mostrado en 2 niveles

A diferencia de RIPng y OSFPv3, IS-IS es capaz de enviar información de *routing* IPv4 e IPv6 a la vez desde un mismo proceso, lo que optimiza el envío de paquetes en una red Doble Pila y el uso de recursos.

A la hora de implementar IS-IS con IPv4 e IPv6 a la vez, hay dos modos de hacerlo:

1. *Single Topology*: IPv4 e IPv6 comparten el cálculo de rutas, se obliga en este modo a que las interfaces IPv4 e IPv6 deben ser las mismas.

2. *Multitopology* [RFC 5120]: el cálculo de rutas es independiente para IPv4 e IPv6 y en este caso se pueden tener distintas topologías para los 2 protocolos, es decir, las interfaces para cada protocolo pueden ser distintas.

IS-IS no usa un *Router ID* de 32 bits como el resto de protocolos, en su lugar, para identificar de forma única los *routers* que hablan IS-IS se usa un direccionamiento propio para identificar de manera única a los *routers* y las áreas.

1.5.5.2 Protocolos EGP

Según la Figura 1.38, los EGP serán protocolos de *routing* dinámico utilizados entre sistemas autónomos para intercambiarse información de rutas entre sí; de esta

forma, cada sistema autónomo anuncia a los demás, cuáles son los prefijos que tiene interiormente y también suelen reenviar información de prefijos de otros sistemas autónomos, esto aplica tanto para prefijos IPv4 como para prefijos IPv6.

En la práctica solo se usa un protocolo, BGP, que para IPv4 utiliza la versión 4 o BGP4 y para IPv6 hay que utilizar el *Multi Protocol BGP* (MBGP) o "BGP4+" que soporta el envío de información de *routing* para distintos protocolos como IPv6 *unicast*, IPv6 *multicast*, VPN de nivel 3, etc. Ver Tabla 1.11.

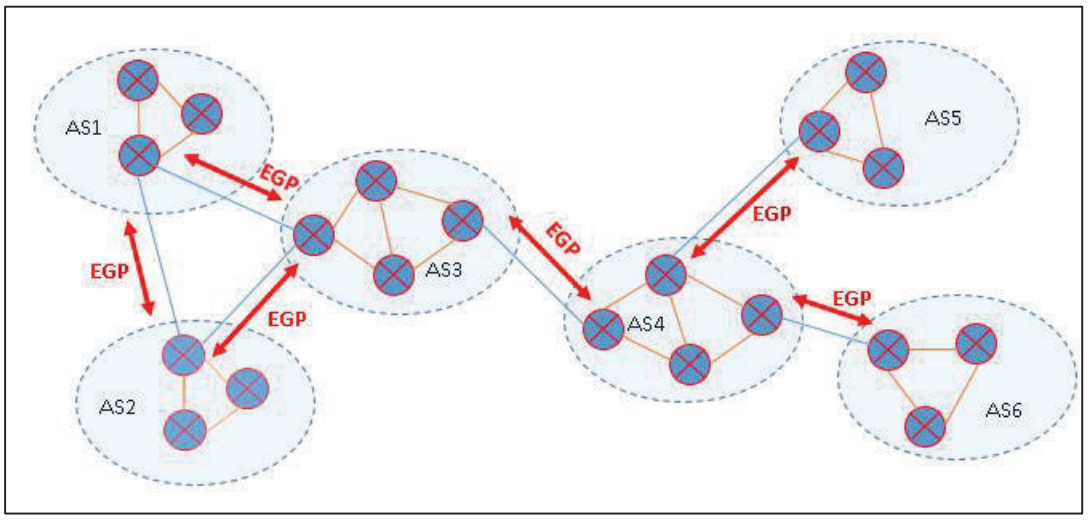


Figura 1.38 EGP entre Sistemas Autónomos

Tabla 1.11 Protocolo para EGP

Tipo	Nombre	IPv4	IPv6	Comentarios
EGP	BGP	BGP4	MBGP	Extendido para soportar IPv6 *Multiprotocol BGP* o BGP4+ soporta *Unicast* IPv6, *Multicast* IPv6, VPN3

1.5.5.2.1 Protocolo BGP

BGP se basa en el PVP (*Path Vector Protocol*) [15] de forma que lo que se envía es la ruta o camino para llegar al prefijo de un sistema autónomo, por ejemplo, para llegar del sistema autónomo 1 al sistema autónomo 2, se indica según la Figura 1.39, que hay que pasar por los sistemas autónomo 5, 9, y 3, en ese orden, es decir que hay 5 saltos.

Figura 1.39 Saltos entre Sistemas Autónomos

BGP es un protocolo orientado a conexión que establece una conexión TCP por el puerto 179 para el intercambio de los siguientes mensajes BGP:

- *OPEN*: Abre una conexión BGP.
- *UPDATE*: Anuncia o confirma un nuevo camino.
- *KEEPALIVE*: en ausencia de *UPDATES* sirve para mantener abierta la conexión TCP y como ACK de un mensaje *OPEN.*
- *NOTIFICATION*: Informa de errores en mensajes precedentes y para cerrar conexiones

Tanto la conexión TCP como los mensajes enviados por BGP son independientes del protocolo de Red y por lo tanto serán iguales para IPv4 e IPv6.

Las consideraciones que son iguales para IPv4 e IPv6 son:

- La mayoría de los atributos BGP como *ORIGIN*, AS-PATH, MED, *LOCAL PREF*, etc, serán iguales para IPv4 e IPv6 ya que tienen significado a nivel de aplicación donde funciona BGP, por ejemplo:, el uso de AS-PATH y su AS *Secuence* serán iguales para IPv4 e IPv6 y se utilizarán en ambos casos para elegir la mejor ruta hacia un prefijo, el que tenga el AS-PATH más corto, o con menos números de sistemas autónomos, y también para prevenir bucles de *routing* ignorando la ruta recibida que incluyan su propio número de sistema autónomo.
- El funcionamiento de eBGP, o exterior BGP, y de iBGP, o interior BGP, será el mismo para IPv4 como para IPv6.

- Existen técnicas de protección de BGP o para asegurar el protocolo BGP que en su mayoría son iguales para IPv4 e IPv6.
- El filtrado de prefijos y el filtrado de prefijos “Bogon”, o que no deberían anunciarse por BGP. Evidentemente los prefijos serán distintos entre IPv4 e IPv6 pero la idea es la misma en ambos casos.

1.5.5.2.2 IPv6 en BGP

En BGP4 solo hay 3 elementos con información específica de IPv4:

1. El atributo *Next-Hop* que se indica mediante una dirección IPv4.
2. *Aggregator* que contiene una dirección IPv4.
3. El NLRI expresado como un prefijo IPv4.

El RFC 4760 que define el *Multiprotocol* BGP, asume que cualquier ruta en BGP tendrá IPv4, que podrá usarse en el atributo *AGGREGATOR*, por lo que para que BGP soporte distintos protocolos de capa de red es necesario únicamente añadir la capacidad de asociar un protocolo de red con los atributos *NEXT-HOP* y NLRI.

Para ello introducen dos nuevos atributos:

1. *Multiprotocol Reachable* NLRI (MP_REACH_NLRI) que indicará la familia de direcciones usadas mediante el *address family identify* (AFI) + el *Next-Hop* de esa familia de direcciones y los prefijos de esa familia que son alcanzables.
2. *Multiprotocol Unreachable* NLRI (MP_UNREACH_NLRI) que solo necesita indicar la familia de direcciones y los prefijos de esa familia de direcciones que dejan de ser alcanzables.

Los tres elementos que suelen necesitar soporte IPv6 son:

1. El transporte de información de *routing*, ya que en MBGP se puede usar una conexión TCP sobre IPv6.

2. Indicar el *Next-Hop* que en MBGP se puede enviar como parte del nuevo atributo MP_REACH_NLRI.

3. Información sobre prefijos IPv6, ya que en MBGP se puede enviar como parte de los nuevos atributos MP_REACH_NLRI y MP_UNREACH_NLRI

Además se deberán aplicar filtros para permitir solamente los prefijos permitidos por una conexión TCP de BGP, así como para evitar prefijos que no deben usarse. La tabla 1.12 muestra los prefijos que no deben usarse.

Tabla 1.12 Prefijos IPv6 que no se deben usar en BGP

Rutas	Prefijos	Comentario
Unspecified Address	::/128	
Loopback Address	::1/128	Se puede agrupar en el prefijo 0000::/8 o mayor
IPv4-mapped Address	::ffff:0.0.0.0/96	
IPv4 compatible Address (Deprecated)	::/96	
Link-Local Addresses	fe80::/10 o mayor	
Site-Local Addresses (Deprecated)	fee0::10 o mayor	
Unique-Local Addresses	fc00::/7 o mayor	
Multicast Addresses	ff00::/8 o mayor	Si no se usa *multicast*
Documentation Address	2001:db8::/32 o mayor	
6Bone Addresses (Deprecated)	3ffe::/16, 5f00::/8	RFCs 1897, 2471, 3701
ORCHID	2001:10::/28	RFC 4843

En este capítulo se estudiaron las bondades que tiene el protocolo IPv6 y las fallas que presentaba IPv4. En el siguiente capítulo se verá la estructura del proveedor de servicios de Internet Ecuaonline S.A.

CAPÍTULO 2

DESCRIPCIÓN DE LA RED ECUAONLINE S.A

2.1 INTRODUCCIÓN

Ecuaonline S.A. es una empresa privada de Telecomunicaciones ubicada en el centro norte de la ciudad de Quito, y brinda actualmente varios servicios en la mayoría del territorio Ecuatoriano.

La empresa por medio de su variedad de aplicaciones comercializa servicios de Telecomunicaciones a sus distintos tipos de clientes, entre ellos se pueden destacar: clientes *home* o considerados como “normales”, los clientes considerados “corporativos” y los clientes “VIP”, todos ellos están clasificados de acuerdo a la capacidad y cantidad de servicios que demandan.

Todos los clientes reciben el servicio contratado por medio de la tecnología de última milla con la que cuenta actualmente la empresa, denominada radio enlace, cuya definición es “Un radioenlace es el conjunto de equipos de transmisión y recepción necesarios para el envío vía radio de una señal de uno a otro nodo o centro de una red” [16] y que trabaja en frecuencias de 2.4 y 5.8 GHz.

Todas las direcciones de Ecuaonline S.A. utilizan IPv4 con el cual, se comercializa todos los servicios que la empresa brinda. Puesto que en un futuro, la comercialización de servicios con el protocolo IPv4 no será posible puesto que en la actualidad se encuentran agotadas todas las direcciones públicas IPv4 que la IANA puede asignar a los RIRs se ve la necesidad imperiosa de migrar a IPv6.

2.2 DESCRIPCIÓN DE LA EMPRESA ECUAONLINE S.A.

ECUAONLINE S.A. es una empresa creada con el objeto de desarrollar aplicaciones, servicios y soluciones IT de última generación para profesionales y empresas en el área de telecomunicaciones.

La compañía está especializada en Consultoría, Dirección Técnica y Ejecución de Proyectos de comunicaciones de Empresa.

Como proveedor de servicios (ISP) y aplicaciones, aporta soluciones integrales de desarrollo, implantación, alojamiento y gestión de aplicaciones: sistemas de gestión de información, *e-comerce*, bases de datos, soluciones de gestión corporativa.

Gracias a todo lo anterior, ECUAONLINE se ha situado en primera línea del sector nacional de las telecomunicaciones, posicionándose como una empresa altamente calificada, innovadora, particularmente preocupada por la calidad y con clara vocación de servicio.

Los principales servicios que ofrece Ecuaonline S.A. se mencionan a continuación:

- *Internet*: Provee este servicio a nivel nacional a clientes corporativos y de pequeños negocios con buena disponibilidad en todo el trayecto de sus enlaces.
- *Interconexión de LAN:* Se emplea para agrandar la red de una empresa desde su oficina matriz hacia sus respectivas sucursales haciéndolo ver como una sola LAN.
- *Voz sobre IP:* Servicio que permite transmisiones de voz a través del Internet.
- *Transferencia de datos:* Permite la transmisión de datos entre LAN.
- *Firewall:* Administración de acceso de usuarios y programas a la LAN.
- *Equipos de alquiler:* El cliente cancela un pago mensual al ISP por el arriendo de equipos como *routers, switches*, antenas, etc.
- *Respaldo de información:* Procedimiento mediante el cual se respaldan los datos de usuario en los servidores del ISP o en una unidad del cliente.

- *Hosting:* Procedimiento mediante el cual se aloja la página *web* del cliente www.ejemplo.com en los servidores de la empresa con la capacidad de manejar información de todo tipo. Tanto el cliente como cualquier persona ajena a la empresa podrá acceder a la página *web* www.ejemplo.com vía Internet.

- *Antispam:* Bloqueo de correo basura "SPAM" con software especializado para este propósito con el fin de reducir el procesamiento de datos en el servidor y así agilizar el envío y recepción de correos.

- *Servidores FTP:* Protocolo especializado para facilitar la administración de contenido en un servidor FTP y permitir el acceso vía *web* con una mayor velocidad de transferencia.

- *Servidor Streeming:* Servidores dedicados exclusivamente para soportar gran cantidad de procesamiento.

- *Antivirus:* Evita el ingreso de código malicioso en sistemas informáticos del usuario final que puedan afectar el funcionamiento y poner en peligro los datos del cliente.

Ecuaonline S.A. tiene cobertura en las principales provincias del territorio Ecuatoriano, la mayor parte de la misma llega al cliente con infraestructura propia, mientras que para sectores alejados se utiliza infraestructura arrendada.

Cuando se utiliza infraestructura propia se realizan los enlaces desde la Matriz ubicada en la ciudad de Quito [17], en el edificio Twin Towers, y llegan hacia el cliente final por medio de enlaces de *backbone* constituido por radio enlaces.

En la Figura 2.1 se muestra un gráfico en donde se encuentran las principales provincias a las que Ecuaonline S.A. presta sus servicios.

La tecnología que Ecuaonline S.A. utiliza para brindar sus servicios, tanto a nivel de backbone como de última milla, se basa en enlaces de radio que en términos de tipos de conexión a Internet se concentran en redes inalámbricas o Wireless.

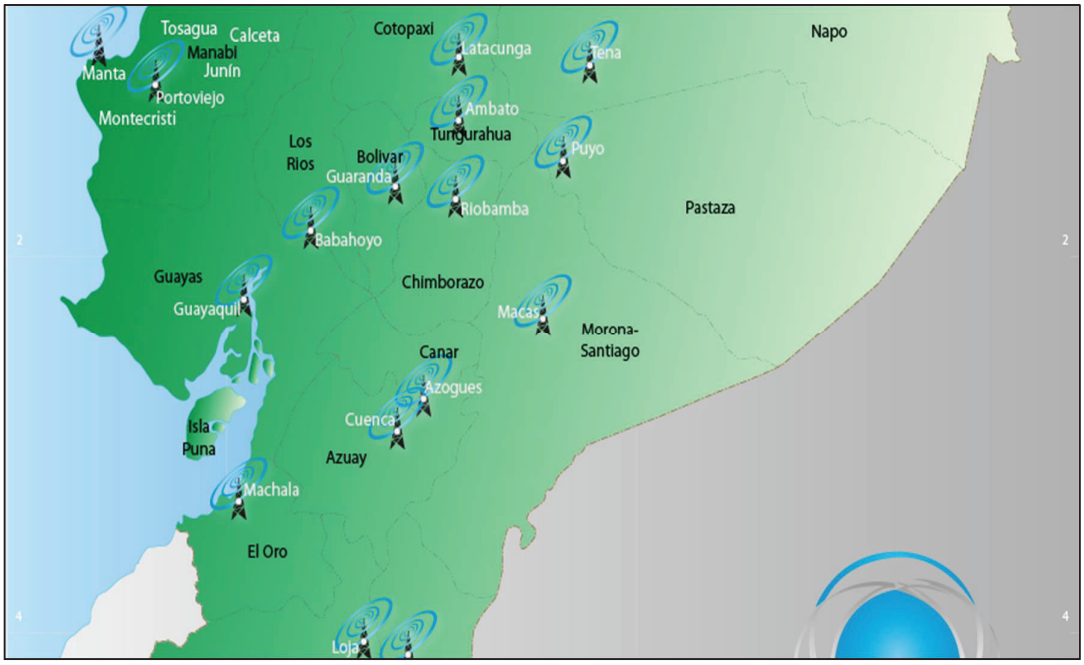


Figura 2.1 Cobertura de Ecuaonline S.A.

Se tienen 2 tipos de redes que se clasifican por su conexión física y se describen a continuación:

1. *Enlace Punto a Punto:* Es aquel que conecta únicamente dos estaciones en un instante dado, ver Figura 2.2. Se pueden establecer enlaces punto a punto en circuitos dedicados o conmutados, que a su vez pueden ser dúplex o half-dúplex.

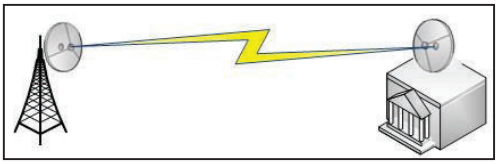


Figura 2.2 Enlace punto – punto.

2. *Enlace Punto a Multipunto:* Según la Figura 2.3 es aquel que conecta más de dos estaciones a la vez.

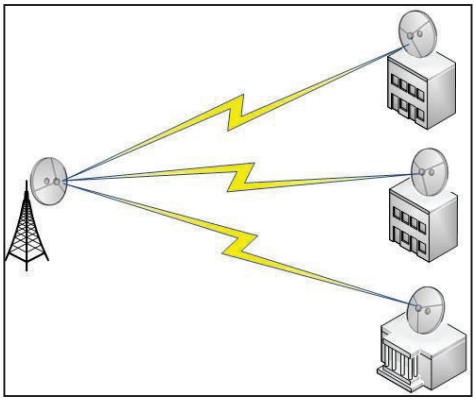


Figura 2.3 Enlace punto – multipunto

2.3 ESTRUCTURA DE LA RED DE ECUAONLINE S.A.

2.3.1 DESCRIPCIÓN DE LA RED METRO *ETHERNET*

Ecuaonline S.A. es una empresa que está constituida como ISP pero que a su vez brinda otros servicios de Telecomunicaciones como transmisión de voz y datos mediante su red Metro *Ethernet*.

El backbone principal está constituido por medio de enlaces de radio punto a punto que utilizan espectro no licenciado (2.4 y 5.8 GHz), los mismos que se encuentran distribuidos estratégicamente para tener una mayor cobertura en todo el territorio ecuatoriano.

Los lugares de difícil acceso, ya sea por el relieve geográfico o por su lejanía, acceden al servicio por medio de terceras empresas (*Carriers*) quienes utilizan infraestructura propia. Las zonas de cobertura se muestran en la Figura 2.1.

2.3.1.1 Descripción de la Capa de *Core*

La red de *Core* o de Borde permite la salida internacional a través de conexiones BGP, entre el *switch* de borde Cisco 3750G y los equipos de los proveedores del servicio de Internet. Actualmente Ecuaonline S.A. cuenta con 1 proveedor de Internet, Claro EC, y un proveedor para navegación local, el NAP EC.

En la Figura 2.4 se puede observar el diagrama de las conexiones de los equipos que conforman la red de *Core* o el borde de la red.

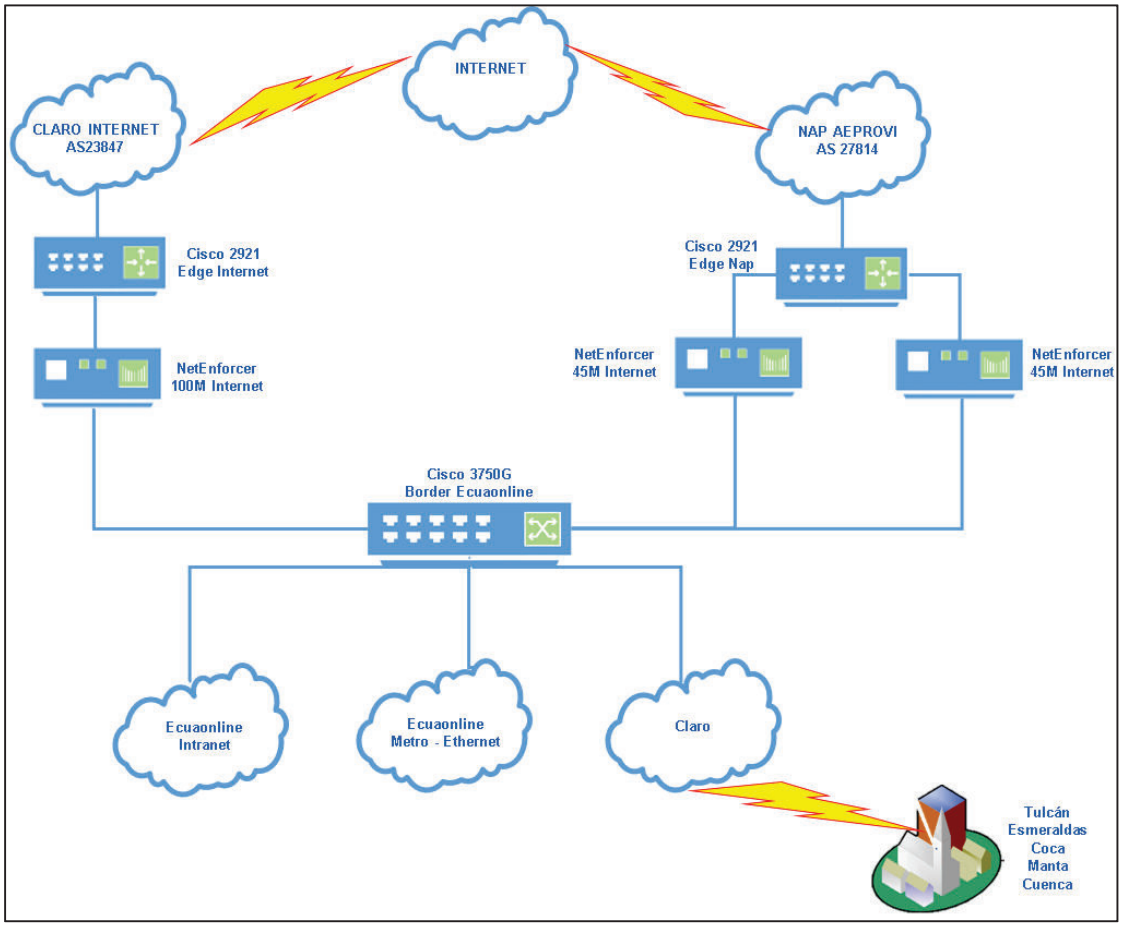


Figura 2.4 Diagrama Esquemático de la Red de *Core*

Ecuaonline S.A. es miembro del NAP.EC que pertenece al AEPROVI[12] logrando con esto mantener un intercambio de tráfico local en la ciudad de Quito entre los proveedores de Internet asociados a esta organización con lo cual optimizan el tiempo de respuesta en todo tipo de tráfico local. La conexión con el NAP.EC se la realiza por medio de una sesión BGP desde un *router* Cisco 2921.

[12] Asociación Ecuatoriano de Proveedores de Internet.

El *switch* de borde Cisco 3750G es un equipo de capa 3 que hace la función de *router* ya que Ecuaonline S.A. no dispone de un *router* de borde con la cantidad de interfaces necesarias para cubrir las necesidades.

La salida de Internet está conformada por 3 equipos administrables:

1. *Router* Edge Internet (x1)
2. NetEnforcer 100M Internet (x1)
3. *Switch* de Borde Internet (x1)

El *router* de Edge se conecta directamente al proveedor de la salida internacional, en este caso Claro EC, y Ecuaonline S.A. anuncia sus prefijos mediante BGP.

El último equipo en la salida a Internet es un Allot NetEnforcer 100M que actúa como Bridge. En términos funcionales el equipo es transparente y no requiere ninguna configuración en particular para dejar pasar el tráfico.

La salida al NAP del Ecuador pasa por 3 equipos administrables:

1. *Router* del NAP (x1)
2. NetEnforcer (x2)
3. *Switch* de borde Internet

El *router* del NAP se conecta directamente al proveedor del mismo, es decir, se conecta directamente a AEPROVI y Ecuaonline S.A. anuncia los prefijos mediante BGP.

Como Ecuaonline no contaba con otro equipo de NetEnforcer 100M, decidió colocar 2 NetEnforcer 45M para balancear la carga enviando por rutas estáticas de diferente peso.

Los 2 NetEnforcer 45M actúan como bridge. En términos funcionales, esos equipos son transparentes y no requieren ninguna configuración en particular para dejar pasar el tráfico. El tráfico que demanda cada cliente se lo controla o limita por medio de los NetEnforcer.

El *switch* de capa 3 (Cisco 3750) permite conectar la intranet de Ecuaonline, el backbone y los equipos de conexión a Internet para otras provincias. En este equipo se configuran VLAN y se asignan rangos de direcciones IP (Privadas y Públicas) a cada uno de los nodos, con lo cual se logra dividir en dominios de *broadcast* la Metro-*Ethernet* de Ecuaonline.

2.3.1.2 Descripción de la Capa Distribución

El *backbone* principal de Ecuaonline, por el cual cursa todo el tráfico, se distribuye en puntos estratégicos de la ciudad de Quito utilizando infraestructura propia, como se observa en la Figura 2.5. Los enlaces son punto a punto con equipos Airmux 400 y Airmux 200 que trabajan en el rango de frecuencias no licenciadas de 5 GHz.

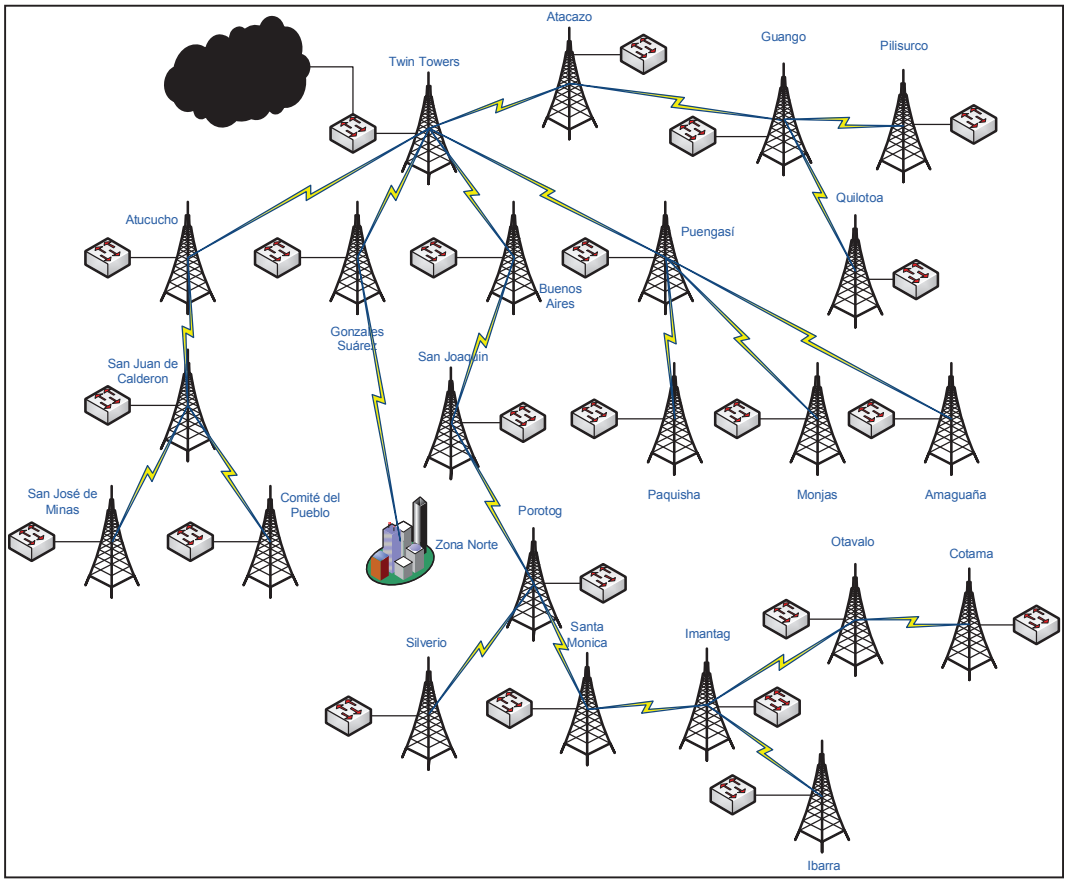


Figura 2.5 Estructura de la red de *backbone*

La ubicación física de los nodos instalados en la ciudad de Quito se detalla en la Tabla 2.1 y la ubicación geográfica se muestra en la Figura 2.6.

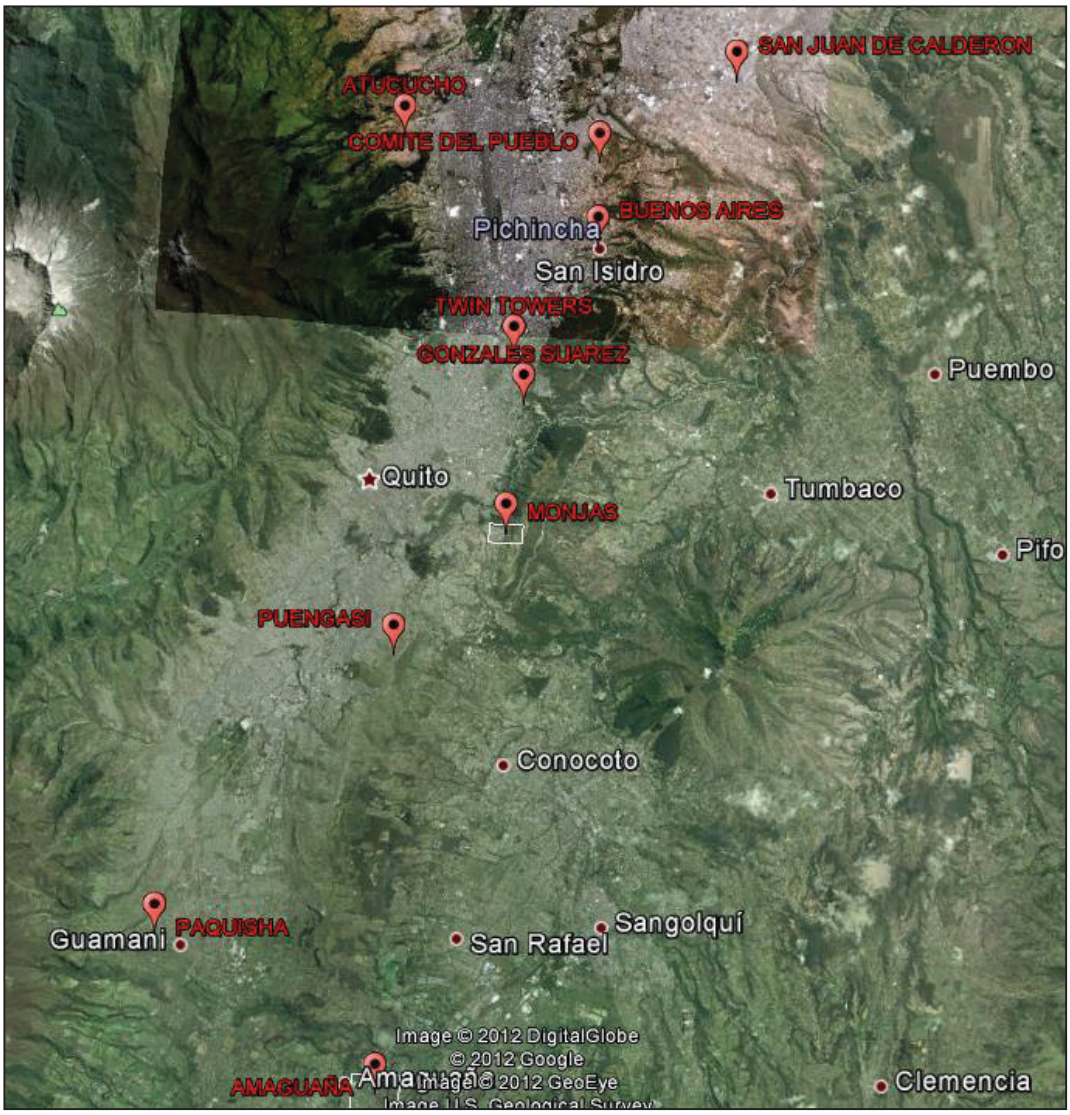


Figura 2.6 Distribución geográfica de los nodos de Quito

Según la Figura 2.6 se ve que en la ciudad de Quito se dispone de 10 nodos distribuidos estratégicamente para brindar los servicios que Ecuaonline S.A. promociona.

Todos los nodos están interconectados para poder llegar a varios rincones dentro de la ciudad de Quito.

Tabla 2.1 Ubicación física de los nodos en la ciudad de Quito

NODO	LATITUD	LONGITUD	ALTURA (m)
Twin Towers	00°10'52"S	78°28'47"W	2784
Atucucho	00°07'26"S	78°30'44"W	2989
Comité del Pueblo	00°07'40"S	78°27'34"W	2892
González Suárez	00°11'38"S	78°28'35"W	2847
Buenos Aires	00°09'01"S	78°27'31"W	2851
San Juan de Calderón	00°06'13"S	78°25'25"W	2663
Puengasí	00°15'48"S	78°30'27"W	3145
Paquisha	00°20'30"S	78°34'03"W	3222
Monjas	00°13'42"S	78º28'28"W	2895
Amaguaña	00°23'15"S	78º29'60"W	2636
San José de Minas	00°10'25"N	78°23'38"W	2382
Atacazo	00°19'06"S	78°36'07"W	3869

La ubicación física de los nodos instalados en la ciudad de Latacunga se detalla en la Tabla 2.2 y la ubicación geográfica se muestra en la Figura 2.7.

Figura 2.7 Distribución geográfica de los nodos de Latacunga

Tabla 2.2 Ubicación física de los nodos en la ciudad de Latacunga

NODO	LATITUD	LONGITUD	ALTURA
Guango	00°53'44.3''S	78°30'5.6''W	3971
Quilotoa	00°53'47''S	78°44'36''W	3893
Pilisurco	01°09'06''S	78°39'59''W	4038

La ubicación física de los nodos instalados en la ciudad de Otavalo se detalla en la Tabla 2.3 y la ubicación geográfica se muestra en la Figura 2.8.

Tabla 2.3 Ubicación física de los nodos en la ciudad de Otavalo

NODO	LATITUD	LONGITUD	ALTURA
Otavalo	00°13'47'' N	78°15'33''W	2547
Cotama	00°14'10.42''N	78°16'6.52''W	2535

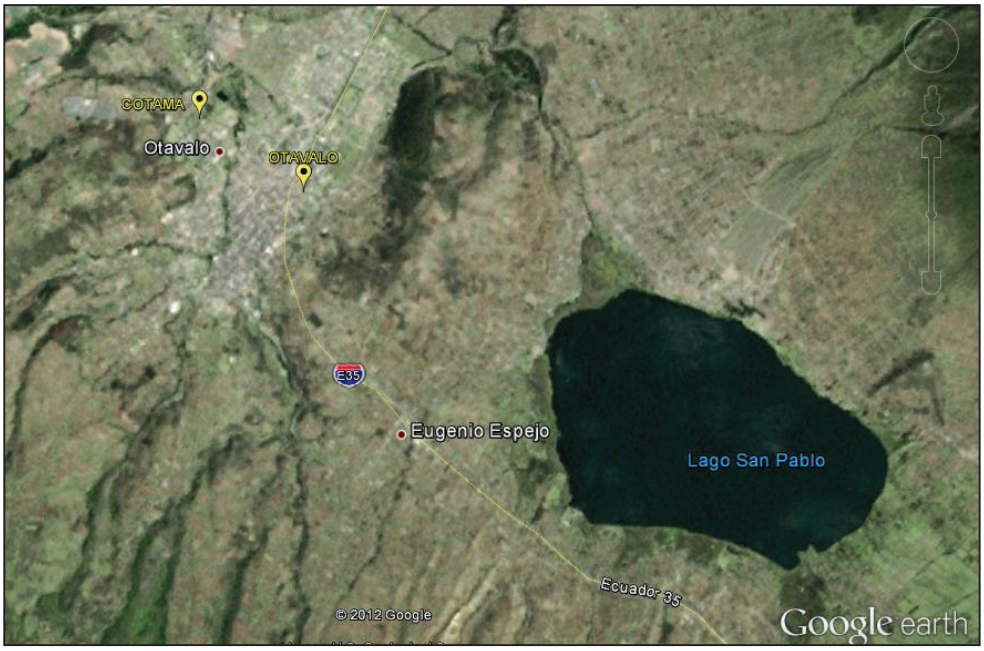


Figura 2.8 Distribución geográfica de los nodos de Otavalo

La ubicación física de los nodos instalados en la ciudad de Ibarra se detalla en la Tabla 2.4 y la ubicación geográfica se muestra en la Figura 2.9.

Tabla 2.4 Ubicación física de los nodos en la ciudad de Ibarra.

NODO	LATITUD	LONGITUD	ALTURA
Imantag	00°21'4,76'' N	78°16'45,32''W	2729
Ibarra	00°20'22'' N	78°05'17''W	2928

Figura 2.9 Distribución geográfica de los nodos de Ibarra

La ubicación física de los nodos instalados en la ciudad de Cayambe se detalla en la Tabla 2.5 y la ubicación geográfica se muestra en la Figura 2.10.

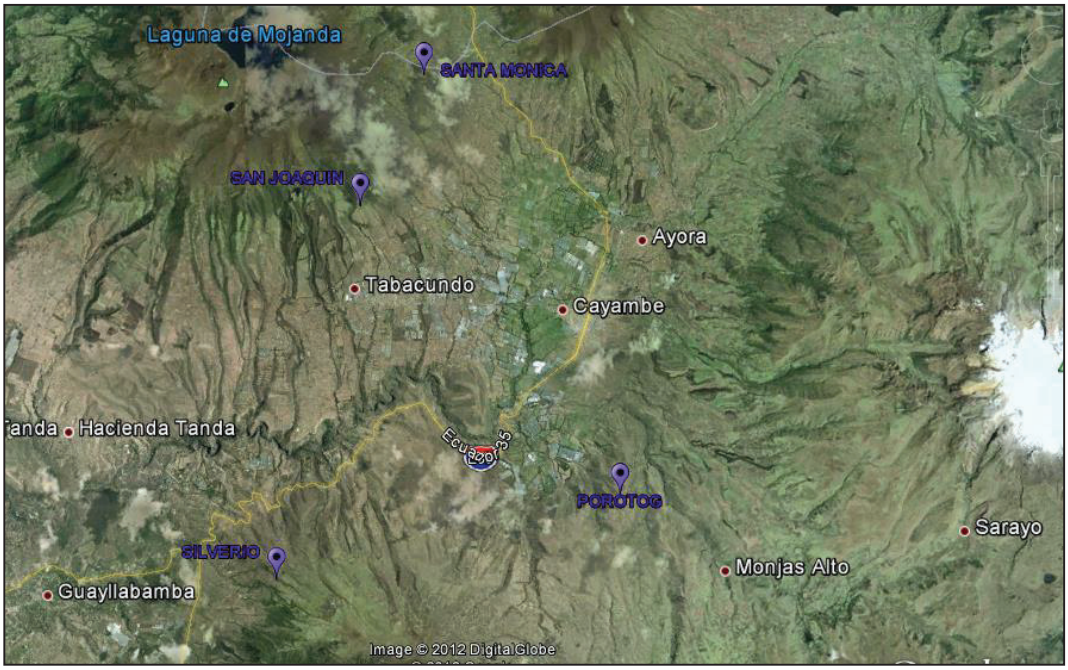


Figura 2.10 Distribución geográfica de los nodos de Cayambe

Tabla 2.5 Ubicación física de los nodos en la ciudad de Cayambe.

NODO	LATITUD	LONGITUD	ALTURA
San Joaquín	00°04'50''N	78°13'40''W	3218
Porotog	00°01'18''S	78°08'10''W	3177
Silverio	00 03'05''S	78°15'26,7''W	3035
Santa Mónica	00°07'35 N	78°12'19''W	3367

2.3.1.2.1 Estructura de los nodos de Ecuaonline S.A.

Cada uno de los nodos está constituido por:

- Una torre de estructura metálica.
- Un inversor CDP (X-Verter) XS3048.
- Un banco de Baterías.
- *Un router* D-Link Dir100.
- Un *switch* Cisco Catalyst 2960.
- Equipos de Radio

La infraestructura de cada nodo está conformada por una torre de estructura metálica, en éste se instalan equipos de radio con el fin de realizar enlaces hacia clientes y otros nodos.

Cada nodo se encuentra equipado con un inversor CDP XS3048 que, conectado a un banco de baterías, evita la interrupción del flujo de energía que es suministrado a los equipos del nodo.

Para hacer un monitoreo remoto del flujo de energía se dispone de un *router* D-Link Dir100 que se conecta directamente a la toma eléctrica del lugar; el equipo tiene en su configuración una dirección de red privada para que al que al conectarlo a uno de los puertos del Catalyst sea un indicador de un posible corte eléctrico.

En la Figura 2.11 se puede observar un diagrama general de la estructura de los nodos.

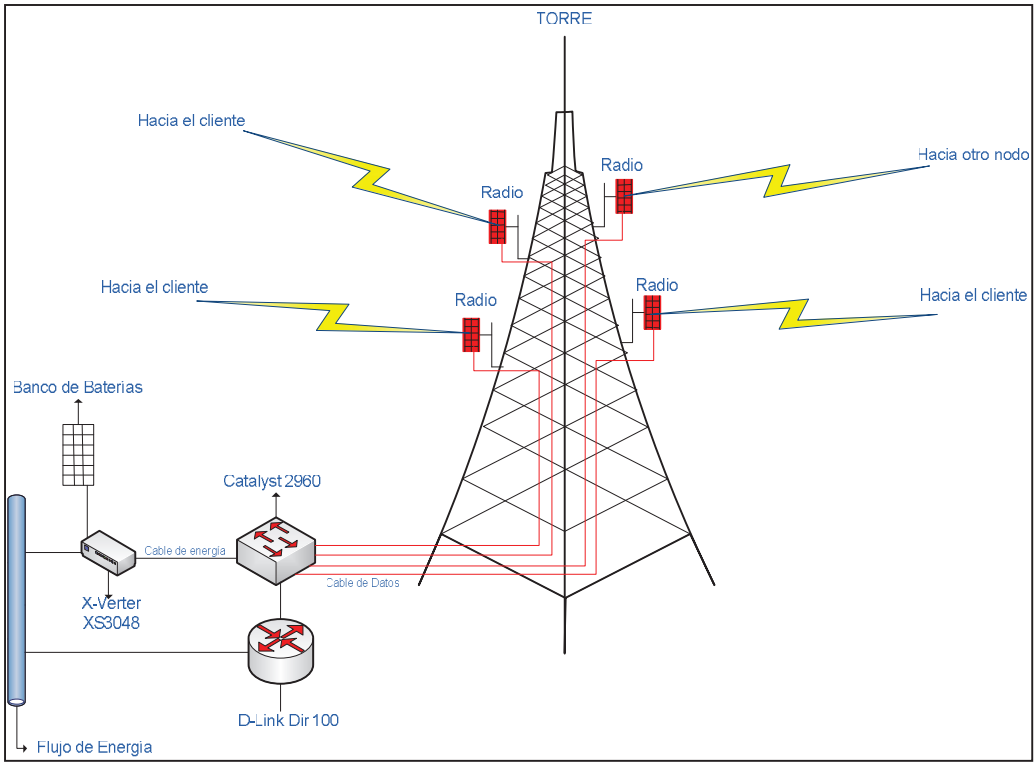


Figura 2.11 Descripción de los nodos de Ecuaonline S.A

2.3.1.3 Descripción de la Capa de Acceso

La red de acceso se encuentra constituida por enlaces de última milla utilizando equipos de radio punto-a-punto y punto-multipunto, los cuales operan en el rango de frecuencias de 2.4GHz o 5.8 GHz.

Para este propósito se utilizan radios de las marcas *Alvarion, Teletronics y Ubiquiti*.

En cada uno de los equipos antes mencionados, se configuran IP privadas, que son asignadas de acuerdo al nodo y ciudad a los que pertenezcan.

A cada cliente se le asigna una IP pública que es configurada en *routers* de propiedad de Ecuaonline S.A. o en equipos finales de propiedad del cliente.

Los *routers* que Ecuaonline S.A. utiliza en los clientes son de marca D-Link y Cisco. En la Figura 2.12 se muestra lo señalado.

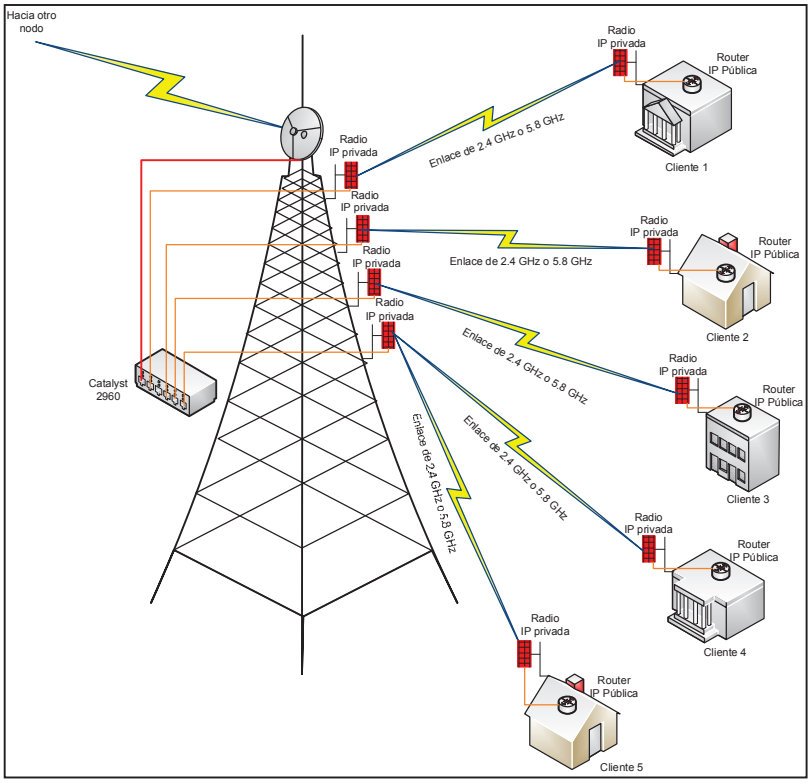


Figura 2.12 Descripción de la capa de Acceso

2.4 EQUIPOS UTILIZADOS EN LA CAPA DE *CORE*, DISTRIBUCIÓN Y ACCESO

En este apartado se presentarán los equipos que conforman la red de *Core* de Ecuaonline S.A.

Cada uno de los equipos serán separados de acuerdo al segmento de red en los que se encuentran, es decir, por ejemplo, dentro de la red de *core* se detallarán los equipos que conforman dicha red. Esto se repite para cada segmento de red.

2.4.1 EQUIPOS DE *CORE*

Aquí se detallarán los equipos que conforman la red de *Core* de Ecuaonline S.A. y que son los que permiten al resto de dispositivos tener salida hacia el mundo, es decir, hacia el Internet.

2.4.1.1 Cisco 2921/K9

Este dispositivo, mostrado en la Figura 2.13, es conocido como *router* de borde dentro de la red de ECUAONLINE S.A. y permite la conexión BGP con Claro [18], la conexión con el NAP.EC y la interconexión entre éstos y la red de distribución. Este equipo tiene soporte para trabajar con IPv6.

Figura 2.13 Cisco 2921/K9

2.4.1.2 Cisco 3750G-24T

El equipo mostrado en la Figura 2.14, es un *switch* de capa 3 administrable que cuenta con la tecnología *Cisco Stack Wise*, una interconexión de pilas de 32 Gbps que permite a los clientes crear un sistema de conmutación unificado y altamente resistente, un *switch* a la vez. Proporciona flexibilidad de configuración, soporte para patrones de red convergentes y automatización de configuraciones de servicios de red inteligentes. Este equipo cuenta con soporte IPv6.

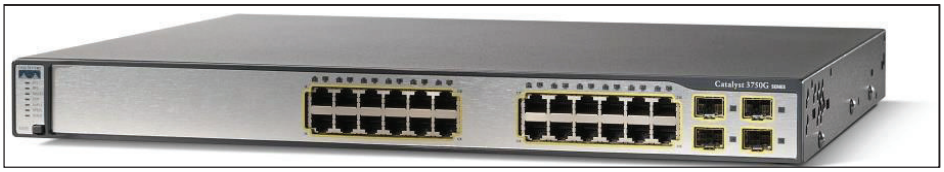


Figura 2.14 Cisco3750G-24T

A este dispositivo se lo conoce como *switch* de capa 3 dentro de la red de Ecuaonline S.A. y permite la conexión entre el *backbone* propio de la empresa con el proveedor Claro, el NAP EC y la intranet de Ecuaonline S.A. En este equipo se configuran VLAN para asignar un rango de direcciones IP tanto privadas como

públicas para cada nodo, consiguiendo de esta manera dividir en dominios de *broadcast* la Metro *Ethernet* de Ecuaonline S.A.

2.4.1.3 NetEnforcer AC 402

El NetEnforcer AC 402, mostrado en la Figura 2.15, es un equipo administrador de ancho de banda que permite conseguir una calidad de servicio (QoS) aceptable y maximizar el rendimiento de las aplicaciones cruciales para la empresa. Los gestores de red deben asignar recursos basados en las prioridades de negocio.

Figura 2.15 NetEnforcer AC-402

NetEnforcer permite asignar el ancho de banda a cada una de las aplicaciones de la red de forma precisa. De esta forma, se garantiza que las transferencias de archivos de gran tamaño no ralenticen las aplicaciones empresariales interactivas, como la planificación de recursos humanos (ERP) o la gestión de la relación con los clientes (CRM), o que el correo electrónico no afecte al rendimiento de VoIP, que no puede retrasarse.

2.4.2 EQUIPOS DE *BACKBONE*

A continuación se detallarán los equipos que conforman el backbone de Ecuaonline S.A.

2.4.2.1 Airmux

Los radios Airmux son dispositivos que según el modelo, ofrecen diferentes características; Como por ejemplo, alcance, velocidad, etc.

2.4.2.1.1 Airmux 200

El Airmux-200, mostrado en la Figura 2.16, es un equipo de radio punto a punto y punto multipunto que combina hasta cuatro E1/T1 y redes *Ethernet* con un alto rendimiento del procesamiento del tráfico sobre frecuencias libres.

Figura 2.16 Equipo Airmux 200

El AirMux-200 tiene una unidad interior (IDU) y una unidad exterior (ODU) conectada mediante un cable *Ethernet* para exteriores Cat-5e que permite una distancia máxima de 100 metros (328 pies) entre las dos unidades.

La unidad para exteriores cuenta con una antena integrada de 22 dBi y se puede usar un conector para antena externa. El alcance máximo de la unidad AirMux-200 es 80 Km (50 millas).

Este dispositivo forma parte del backbone de Ecuaonline S.A., y actualmente es utilizado como enlace punto a punto para conectar los siguientes nodos:

- Twin Towers – González Suárez.
- Twin Towers – Atucucho.
- Atucucho – San Juan de Calderón.
- Twin Towers – Puengasí.
- Puengasí – Monjas

2.4.2.1.2 Airmux 400

El Airmux-400, que se muestra en la Figura 2.17, presta servicios *Ethernet* y TDM sobre un único enlace inalámbrico en varias frecuencias inferiores a 6 GHz, que incluyen 2.4 GHz, 4.8 GHz, 4.9 GHz y 5.x GHz.

Tiene 16 interfaces E1/T1 y hasta tres puertos *Ethernet*. El dispositivo Airmux-400 opera en topologías punto a punto y punto multipunto que soportan un rendimiento neto en full duplex de 100 Mbps (velocidad de datos en el aire de 200 Mbps) para distancias de hasta 120 Km (74.5 millas).

Este dispositivo forma parte del *backbone* de la red de Ecuaonline S.A. Es utilizado como enlace punto a punto para conectar los siguientes nodos:

- Twin Towers – Buenos Aires.
- Twin Towers – Atacazo.

Figura 2.17 Airmux – 400.

2.4.2.2 Teletronics TT5800

El equipo que se muestra en la Figura 2.18, conocido como radio Teletronics TT5800, presta servicios *Ethernet* y TDM sobre un único enlace inalámbrico operando en el rango de frecuencias no licenciadas de los 5.8 GHz.

El Teletronics TT5800 es capaz de trabajar en topologías punto a punto y punto multipunto en las modalidades de bridge y AP. El modo bridge es totalmente transparente y permite el paso de direcciones MAC ilimitadamente.

Cuenta con encriptación WEP y administración del equipo basado en *web*. La velocidad de transferencia es de 54 Mbps y la distancia depende de las antenas externas que se utilicen. El equipo cuenta con una potencia de salida de 200 mW.

Figura 2.18 Teletronics TT5800

En la red de Ecuaonline S.A. se lo utiliza para conectar cuatro nodos por los que no circula mayor cantidad de tráfico, debido a que las características de los mismos son suficientes para transportar los servicios contratados por el cliente. Los nodos son:

- Puengasí – Paquisha.
- Puengasí – Amaguaña.
- San Juan de Calderón – San José de Minas.
- San Juan de Calderón – Comité del Pueblo.

2.4.2.3 Catalyst 2960 24TT-L

El equipo mostrado en la Figura 2.19, es un *switch* de 24 puertos que se encuentra en todos los nodos que tiene el proveedor.

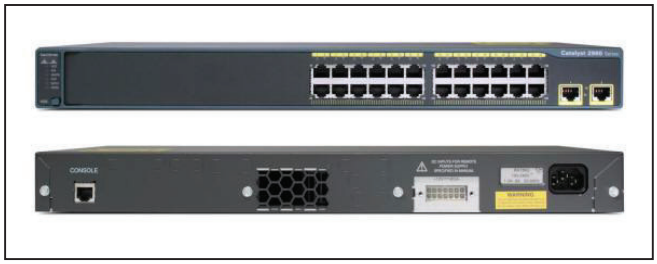


Figura 2.19 Catalyst 2960 24TT-L

La función principal es interconectar el nodo principal con los clientes por medio de radio enlaces, además permite administrar los enlaces de los nodos y los equipos conectados al mismo.

2.4.2.4 Inversor CDP (X-Verter) XS3048

Este equipo, que se observa en la Figura 2.20, está diseñado para satisfacer la demanda de energía eléctrica cuando se presentan cortes del flujo eléctrico constante o esporádicamente.

Cuenta con un regulador automático de voltaje que estabiliza el flujo cuando éste se encuentra por encima o por debajo de las condiciones normales de trabajo.

Figura 2.20 Inversor X-Verter XS3048.

El equipo, proporciona respaldo de energía a todos los equipos de los nodos de Ecuaonline S.A. cuando exista falla o suspensión temporal en el suministro de energía eléctrica normal. Cada nodo tiene un respaldo de baterías de 12 horas.

2.4.2.5 *Router* D-Link DIR-100

El equipo que se observa en la Figura 2.21, es un *router* sencillo que puede ser administrado vía *web*. Brinda QoS, proporciona prioridad en la transmisión y la recepción de los paquetes de Voz sobre IP (VoIP), a través de Internet, mejorando la calidad de las llamadas telefónicas a través de este medio. Además, permite a los usuarios experimentar ventajas en el uso de aplicaciones de multimedia y juegos *on-line* sobre Internet, sin la preocupación de producir congestión de tráfico.

Figura 2.21 Router D-Link DIR-100

Este equipo forma parte de cada nodo de la red de backbone de Ecuaonline S.A. y es utilizado especialmente para alertar por fallas en el suministro eléctrico con lo cual se pueden tomar las medidas que sean necesarias para solucionar el inconveniente.

2.4.3 EQUIPOS DE ACCESO

En esta sección se presentan todos los equipos que Ecuaonline S.A. utiliza para conformar el trayecto de última milla.

2.4.3.1 Ubiquiti

Las alternativas en equipos de la línea Ubiquiti y que son utilizados por Ecuaonline S.A. se presentan a continuación.

2.4.3.1.1 Nanobridge M5

El equipo que se presenta en la Figura 2.22, cuenta con una antena MIMO de ganancia de 22 dBi, la frecuencia de funcionamiento está en el rango de los 5475 MHz hasta los 5825 MHz. Dispone de indicadores LED de actividad y nivel de señal para facilitar la tarea de los instaladores. La protección mejorada contra subidas de tensión del *Ethernet* y RF permite un funcionamiento prolongado incluso en los entornos más duros. Elevado rendimiento, AirMax y compatible con *AirControl*. Hasta 150 Mbps reales de rendimiento y un alcance de máximo 20 Km, con polarización dual (vertical y horizontal).

Figura 2.22 Nanobridge M5

2.4.3.1.2 Bullet M5

El equipo que se observa en la Figura 2.23, cuenta con tecnología MIMO, permite llegar hasta 100 Mbps, logrando ser muy útil en aplicaciones de grandes distancias, ofrece un alcance de hasta 50 Km. Es un radio AP/CPE/WDS completo con conector N-Macho para conexión directa a cualquier antena sin pérdidas por *pigtails*, ni problemas de montaje. Se alimenta a través del cable *Ethernet* (PoE) donde también se llevan los datos a o desde el radio.

Su configuración y monitoreo es simple y fácil a través de un navegador *web*. Puede conectarse a antenas omnidireccionales o sectoriales para proveer servicio multipunto en el rango de frecuencias de los 5 GHz. Los datos y la alimentación son recibidos/enviados a través de un único cable UTP.

Figura 2.23 Bullet M5

2.4.3.1.3 Nanostation 5

El equipo que se muestra en la Figura 2.24, es una unidad de radio 802.11a, que opera en frecuencias en el rango de los 5.4 Ghz, con una antena integrada de 14 dBi con polarización doble (vertical y horizontal) para interiores y exteriores, con lo cual permite ser cliente *bridge* o un cliente punto de acceso (AP). Tiene una potencia de 26 dBm y una sensibilidad de 97 dBm. Con un alcance de hasta 5 Km.

Los esquemas de modulación relacionados con la norma 802.11a y su potente radio de 250 mW permite alcanzar velocidades de hasta 54 Mbps, auto ajustándose a distancias en forma automática o manual logrando comunicaciones estables de hasta 6 Km.

Figura 2.24 Nanostation 5

2.4.3.1.4 Powerstation 5

El equipo que se muestra en la Figura 2.25, es una unidad de radio 802.11a, que opera en frecuencias en el rango de los 5.15 - 5.85 GHz, con una antena integrada

de 22 dBi, con polarización doble (vertical y horizontal) para exteriores, puede ser utilizado como un AP o *Bridge*. Con un alcance de hasta 50 Km y puede proporcionar un rendimiento significativamente mayor (hasta 50 Mbps).

Figura 2.25 Powerstation 5

2.4.3.2 Alvarion Breeze Access VL 5.8

Breeze Access VL es la plataforma inalámbrica de banda ancha de Alvarion en la frecuencia de 5 GHz (cubre toda la banda de 5 GHz). Tiene características, tales como, enlace fuera de la línea de vista (NLOS), alcance extendido, alta capacidad en todos los tamaños de paquete, cifrado y Calidad de Servicio (QoS) de extremo a extremo para aplicaciones donde el tiempo es crítico.

Soporta la concurrencia de multi-frecuencias con velocidades de abonado de 3 a 54 Mbps. Además, consta de antena integrada de abonado de 21 dBi con polarización doble (horizontal y vertical).

Estos equipos son utilizados para enlaces punto a multipunto, con lo que se tienen dos componentes del enlace:

2.4.3.2.1 Unidades de Acceso (AU)

El equipo mostrado en la Figura 2.26 es instalado en el sitio de la estación base (en el nodo de la red de Ecuaonline S.A.); cada AU incluye una unidad interna y una externa. La interna se conecta con la red mediante una interfaz estándar *Ethernet* 10/100 BaseT (RJ-45), y la unidad externa se conecta con la unidad interna mediante un cable CAT-5. Con la estación base se pueden utilizar diversas antenas: 360,120, 60 y 90 grados.

Figura 2.26 Unidad de acceso Alvarion

2.4.3.2.2 Unidades de Abonado (SU)

La unidad de abonado (SU) que se muestra en la Figura 2.27, permite al cliente la conexión con la estación base, y puede soportar un usuario único o múltiples usuarios.

Figura 2.27 Unidad de abonado Alvarion

Las unidades de abonado proveen una plataforma eficiente para Internet e Intranet de alta velocidad, con servicios de VoIP, VPN, entre otros. Cada SU se conecta con la red mediante una interfaz estándar *Ethernet*10/100 BaseT (RJ-45), y se conecta con la unidad interna mediante un cable CAT-5.

2.4.4 EQUIPOS DE USUARIO

Como equipos finales se utilizan *routers* de la marca CISCO y D-Link, éstos son asignados de acuerdo a los requerimientos de servicio del cliente, en el caso de necesitarse una red privada de datos, además del servicio de Internet, VoIP y/o calidad de servicio (QoS). Los equipos utilizados son:

- Router Cisco 2610, que se muestra en la Figura 2.28.

Figura 2.28 Cisco 2610

- Router Cisco 1721, que se observa en la Figura 2.29.

Figura 2.29 Cisco 1721

- Router Cisco 1711, que se presenta en la Figura 2.30.

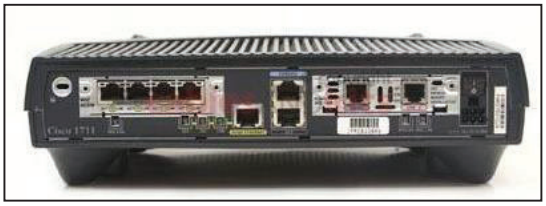


Figura 2.30 Cisco 1711

Cuando se contrata únicamente el servicio de Internet, se instalan equipos de la marca D-Link, de los modelos que se presentan a continuación:

- Router Dir-100 que se observa en la Figura 2.31.

Figura 2.31 D-Link DIR-100

- Router Dir-600, que se muestra en la Figura 2.32.

Figura 2.32 D-Link DIR-600

2.5 DISTRIBUCIÓN DE LOS CLIENTES DE ECUAONLINE S.A.

2.5.1 CLIENTES DE LA CIUDAD DE QUITO

Los clientes actuales y futuros de la ciudad de Quito que obtienen o desean obtener acceso a un servicio específico, de Ecuaonline S.A., deberán tener línea de vista hacia un nodo cercano de la empresa para poder realizar un enlace de radio y así obtener el servicio requerido. Tanto el número de clientes, nodos involucrados, tipo

de servicio contratado y tipo de equipos se muestra en la Tabla 2.6. Una ampliación a la tabla se muestra en el Anexo 1, Tabla A-1.

Tabla 2.6 Distribución de los clientes de Ecuaonline S.A en la ciudad de Quito

NOBRE DEL NODO	NÚMERO DE CLIENTES	USUARIOS CON SERVICIO DE INTERNET	USUARIOS CON SERVICIO DE DATOS	EQUIPOS	
TWIN TOWERS	18	18	3	CISCO 1711	16
				CISCO 2610	2
BUENOS AIRES	20	20	4	CISCO 1711	15
				CISCO 2610	2
				DLINK DIR 600	2
				CISCO 1721	1
GONZÁLEZ SUÁREZ	25	25	6	CISCO 1711	17
				CISCO 2610	3
				DLINK DIR 600	3
				CISCO 1721	2
ATUCUCHO	16	16	8	CISCO 1711	9
				CISCO 2610	2
				DLINK DIR 600	2
				CISCO 1721	3
SAN JUAN DE CALDERÓN	26	26	7	CISCO 1711	14
				CISCO 2610	1
				DLINK DIR 600	6
				CISCO 1721	5
COMITÉ DEL PUEBLO	2	2	1	CISCO 1711	1
				CISCO 2610	1
PUENGASÍ	14	14	1	CISCO 1711	7
				CISCO 2610	1
				DLINK DIR 600	6
MONJAS	1	1	1	CISCO 1721	1
PAQUISHA	2	2	1	CISCO 1711	1
				CISCO 2610	1
AMAGUAÑA	1	1	0	CISCO 1711	1

2.5.2 CLIENTES DE LA CIUDAD DE LATACUNGA

Los clientes de la ciudad de Latacunga se encuentran distribuidos de acuerdo a la Tabla 2.7. Una ampliación a la tabla se muestra en el Anexo 1, Tabla A-2.

Tabla 2.7 Distribución de los clientes de Ecuaonline S.A en la ciudad de Latacunga

NOBRE DEL NODO	NÚMERO DE CLIENTES	USUARIOS CON SERVICIO DE INTERNET	USUARIOS CON SERVICIO DE DATOS	EQUIPOS	
QUILOTOA	26	26	2	CISCO 1711	18
				DLINK DIR 600	8
GUANGO	27	27	7	CISCO 1711	19
				CISCO 2610	3
				DLINK DIR 600	5
PILISURCO	5	5	3	CISCO 1711	3
				CISCO 2610	1
				CISCO 1721	1

2.5.3 CLIENTES DE LA CIUDAD DE IBARRA

Los clientes de la ciudad de Ibarra se encuentran distribuidos de acuerdo a la Tabla 2.8. Una ampliación a la tabla se muestra en el Anexo 1, Tabla A-3.

Tabla 2.8 Distribución de los clientes de Ecuaonline S.A en la ciudad de Ibarra

NOBRE DEL NODO	NÚMERO DE CLIENTES	USUARIOS CON SERVICIO DE INTERNET	USUARIOS CON SERVICIO DE DATOS	EQUIPOS	
IMANTAG	17	17	8	CISCO 1711	6
				CISCO 2610	1
				DLINK DIR 600	3
				CISCO 1721	7
IBARRA	18	18	10	CISCO 1711	6
				CISCO 2610	7
				DLINK DIR 600	4
				CISCO 1721	1

2.5.4 CLIENTES DE LA CIUDAD DE OTAVALO

Los clientes de la ciudad de Otavalo se encuentran distribuidos de acuerdo a la Tabla 2.9. Una ampliación a la tabla se muestra en el Anexo 1, Tabla A-4.

Tabla 2.9 Distribución de los clientes de Ecuaonline S.A en la ciudad de Otavalo

NOBRE DEL NODO	NÚMERO DE CLIENTES	USUARIOS CON SERVICIO DE INTERNET	USUARIOS CON SERVICIO DE DATOS	EQUIPOS	
COTAMA	9	9	3	CISCO 1711	6
				CISCO 2610	1
				DLINK DIR 600	2

2.5.5 CLIENTES DE LA CIUDAD DE CAYAMBE

Los clientes de la ciudad de Cayambe se encuentran distribuidos de acuerdo a la Tabla 2.10. Una ampliación a la tabla se muestra en el Anexo 1, Tabla A-5.

Tabla 2.10 Distribución de los clientes de Ecuaonline S.A en la ciudad de Cayambe

NOBRE DEL NODO	NÚMERO DE CLIENTES	USUARIOS CON SERVICIO DE INTERNET	USUARIOS CON SERVICIO DE DATOS	EQUIPOS	
SAN JOAQUÍN	14	14	5	CISCO 1711	9
				CISCO 2610	1
				DLINK DIR 600	1
				CISCO 1721	3
SILVERIO	4	4	2	CISCO 1711	1
				DLINK DIR 600	1
				CISCO 1721	2
POROTOG	17	17	2	CISCO 1711	14
				CISCO 2610	1
				DLINK DIR 600	1
				CISCO 1721	1
SANTA MÓNICA	8	8	3	CISCO 1711	4
				DLINK DIR 600	1
				CISCO 1721	3

2.6 DISTRIBUCIÓN DE LA RED INTERNA DE ECUAONLINE S.A.

La red interna de Ecuaonline S.A. se encuentra distribuida como se muestra en la Figura 2.33. Aquí se encuentran equipos de Gerencia, Ventas, Contabilidad, Desarrollo, Monitoreo y Departamento Técnico. Por otra parte y dentro de la

estructura de la red hay el cuarto de servidores en donde se conectan todos los equipos con este propósito para brindar diferentes tipos de servicios a los clientes de la empresa. Aquí se encuentran servidores de DNS, Anti-Spam, correos y aplicaciones.

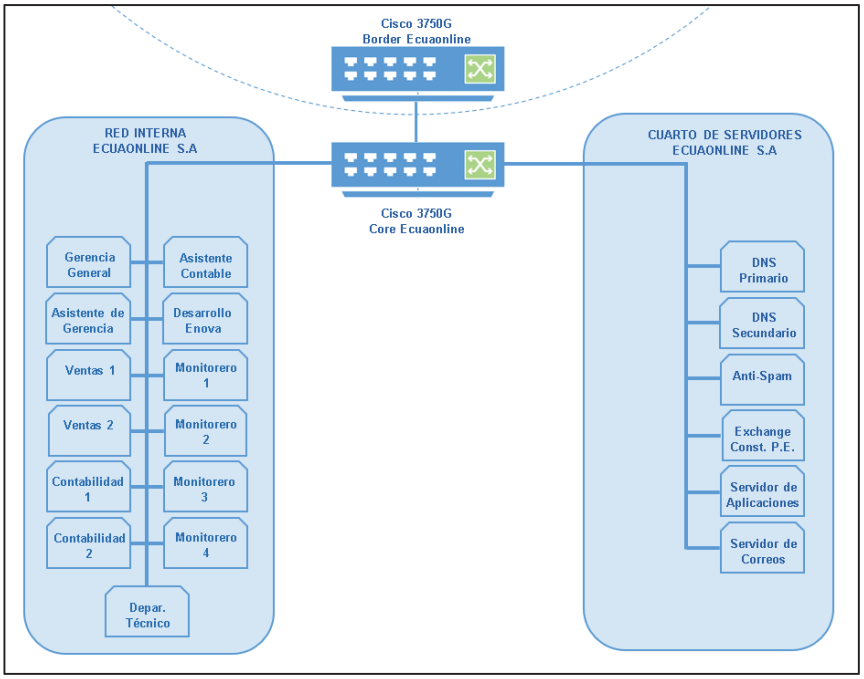


Figura 2.33 Descripción de la red interna de Ecuaonline S.A

2.7 *POOL* DE DIRECCIONES IPv4 DE ECUAONLINE S.A.

Ecuaonline S.A. tiene dos *pools* de direcciones IPv4 solicitados directamente a LACNIC para su uso interno, es decir, para poder entregar a los clientes IP públicas y de esta manera brindar el servicio público a cada usuario.

LACNIC muestra directamente los *pools* del proveedor consultando por IP o por AS. El Sistema Autónomo de Ecuaonline S.A. es el AS27868. Ver Figura 2.34.

En la Tabla 2.11, se presenta el *pool* 190.123.0.0/20 en donde indica que se trata de una dirección Pública IPv4 clase B con 4094 posibles direcciones públicas a asignar (2^{12}-2). El rango de direcciones va desde la 190.123.0.1 hasta la 190.123.15.254.

En la Tabla 2.11 se muestra información importante al trabajar con IPv6, ya que indica que la dirección mapeada IPv4 para IPv6 es ::ffff:be7b:0000 y además que el prefijo 6to4 es 2002:be7b:0000::/48. Esta información es fundamental cuando se requiera trabajar con mecanismos de transición IPv4 a IPv6.

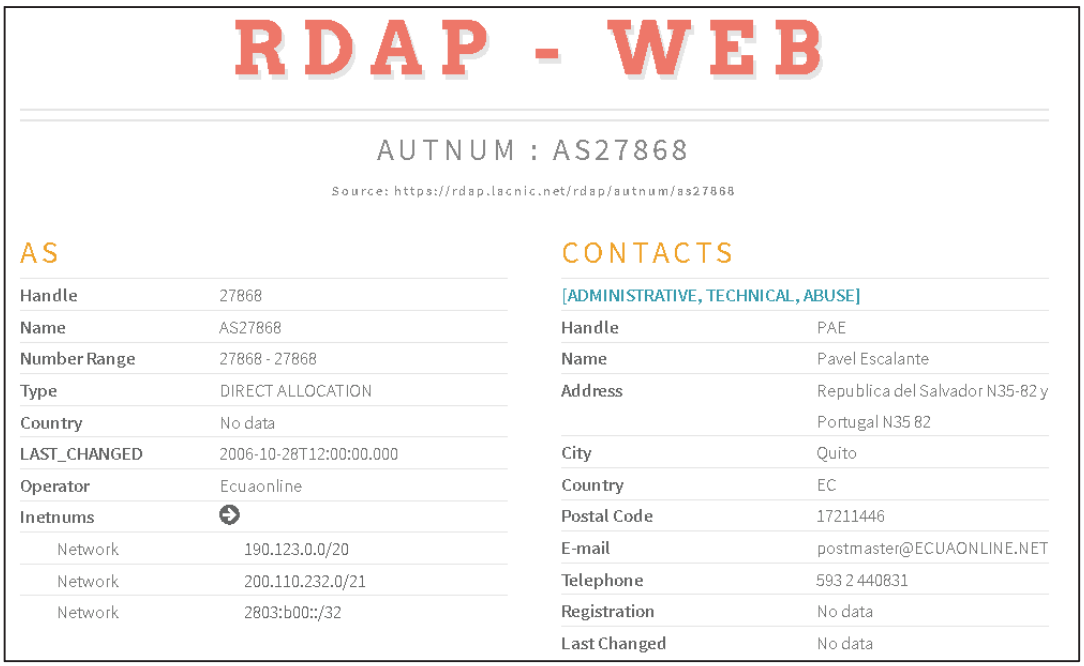


Figura 2.34 Consulta de redes de Ecuaonline S.A. en la página de LACNIC

Tabla 2.11 *Pool* 190.123.0.0/20

IP *address*	190.123.0.0
class	B
type	*PUBLIC*
network	190.123.0.0
bitmask	20
netmask	255.255.240.0
wildcardmask	0.0.15.255
host range	190.123.0.1-190.123.15.254
broadcast address	190.123.15.255
total IP addresses	4094
short	190.123.0/20
mapped IPv4 address	::ffff:be7b:0000
6to4 prefix	2002:be7b:0000::/48

En la Tabla 2.12, se muestra el *pool* 200.110.232.0/21 en donde indica que se trata de una dirección Pública IPv4 clase B con 2046 posibles direcciones públicas a asignar (2^{11}-2). El rango de direcciones va desde la 200.110.232.1 hasta la 200.110.239.254.

Tabla 2.12 *Pool* 200.110.232.0/21

IP address	200.110.232.0
class	C
type	*PUBLIC*
network	200.110.232.0
bitmask	21
netmask	255.255.248.0
wildcardmask	0.0.7.255
host range	200.110.232.1- 200.110.239.254
broadcast address	200.110.239.255
total IP addresses	2046
mapped IPv4 address	::ffff:c86e:e800
6to4 prefix	2002:c86e:e800::/48

En la Tabla 2.12 se muestra información importante cuando se trabaje con IPv6, ya que indica que la dirección mapeada IPv4 para IPv6 es ::ffff:c86e:e800 y además que el prefijo 6to4 es 2002:c86e:e800::/48. Esta información es fundamental cuando se requiera trabajar con mecanismos de transición IPv4 a IPv6.

Con toda esta descripción proporcionada de la red Ecuaonline S.A se procederá a realizar el diseño en el capítulo 3 de la red IPv6 para dar el servicio de Internet a los usuarios de Quito, Latacunga, Cayambe, Otavalo e Ibarra.

CAPÍTULO 3

DISEÑO DE LA RED PORTADORA DE TELECOMUNICACIONES

Ya se mencionó que en primer lugar se busca una transición amigable en coexistencia con IPv4, donde amigable significa que no se debe afectar a lo que ya estaba funcionando: una gran infraestructura basada en IPv4.

Para esto se analizaron 3 estrategias:

1. Usar IPv6 Nativo
2. Encapsulado o túneles
3. Estrategia de traducción

En este capítulo se explica sobre el diseño y planificación de la transición hacia IPv6 que incluirá, establecer una estrategia, mecanismos de transición a utilizar, plan de numeración, y la conexión IPv6.

A priori se ha considerado que en la mayoría de los casos, la mejor estrategia es usar Doble Pila como mecanismo de transición, es decir, IPv4 e IPv6 a la vez en la red.

3.1 VERIFICACIÓN DE EQUIPOS

Tal como se citó en el capítulo 2, Ecuaonline S.A. es un proveedor de servicios de Internet con cobertura en las ciudades de Quito, Latacunga, Cayambe, Otavalo e Ibarra. Utiliza la tecnología inalámbrica en las bandas 2.4 y 5.8 GHz para el acceso hacia el cliente. Entre las tecnologías que se utiliza en la red están: equipos *Cisco, NetEnforcer, Alvarion, Ubiquiti Networks, Airmux, Teletronics y Dlink.*

Para llevar a cabo el diseño de la red IPv6 en Ecuaonline S.A. se requiere conocer si los equipos que están en las redes de *Core*, Distribución y Acceso soportan la nueva tecnología.

En la Tabla 3.1 se presentan los equipos que conforman la Red de *Core* y Borde. En esta red hay 7 equipos de *networking*, 13 equipos de usuario y 2 *servers* físicos que tienen virtualizadas máquinas virtuales.

Todos los equipos indicados en la Tabla 3.1 soportan IPv6 en Doble Pila a excepción de los 3 NetEnforcer AC-402 que se deberían reemplazar para que el diseño en IPv6 Nativo funcione.

Tabla 3.1 Equipos de *Core* Ecuaonline S.A.

CORE						
EQUIPO	**MODELO**	**CAPA**	**IOS INSTALADO**	**SOPORTE IPv6**	**IOS MÍNIMO PARA SOPORTE IPv6**	**CANTIDAD**
ROUTER	CISCO 2921/K9	3	15.0(1)M2	SI	15.0(1)M2	**2**
SWITCH	CISCO WS-C3750G-24T	3	12.2(25)SEE	SI	12.2(2)T	**2**
NETENFORCER	AC-402	3	SNE400	NO	N/A	**3**
CLON	*CORE* I5	7	WIN 7	SI	WIN 7	**13**
SERVER	HP-DL360P	7	SERVER 2008	SI	SERVER 2000	**1**
SERVER	CENTOS	7	CENTOS	SI	CENTOS	**1**

En la Tabla 3.2 se presentan los equipos que conforman la Red de distribución. En esta red hay 44 equipos de *networking* y 22 radios de comunicaciones.

Todos los equipos de capa 3 indicados en la Tabla 3.2 no soportan IPv6 en Doble Pila. Pero para el diseño no es esencial, ya que los *routers* D-Link DIR 100 únicamente son utilizados para alertar posibles fallas eléctricas en el lugar.

Todos los radios de esta red son de capa 1 y 2, por tal razón, el tráfico que transporten es independiente de IPv4 o IPv6. Para este diseño se ha pensado utilizar una red de distribución que sea capaz de soportar IPv6 en la capa de red, es decir, se busca utilizar equipos capa 3 en este segmento de red, para tener la capacidad de trabajar en Doble Pila, para ello, se deberá buscar la mejor opción de equipos de radio con soporte en IPv6.

Tabla 3.2 Equipos de Distribución Ecuaonline S.A.

DISTRIBUCIÓN						
EQUIPO	**MODELO**	**CAPA**	**IOS INSTALADO**	**SOPORTE IPv6**	**IOS MÍNIMO PARA SOPORTE IPv6**	**CANTIDAD**
RADIO	AIRMUX 400	2		N/A	N/A	**4**
RADIO	AIRMUX 200	2		N/A	N/A	**10**
ROUTER	D-LINK DIR 100	3	403WWB13	N/A	N/A	**22**
SWITCH	WS-C2960-24TT-L	2	12.2(35)SE5	N/A	N/A	**22**
RADIO	TELETRONICS TT 5800	2		N/A	N/A	**8**

En la Tabla 3.3 se presentan los equipos que conforman la Red de Acceso. En esta red hay 270 equipos de *networking*, y 540 radios de comunicaciones.

Tabla 3.3 Equipos de Acceso Ecuaonline S.A

ACCESO						
EQUIPO	**MODELO**	**CAPA**	**IOS INSTALADO**	**SOPORTE IPv6**	**IOS MÍNIMO PARA SOPORTE IPv6**	**CANTIDAD**
ROUTER	CISCO 2610	3	12.3(1)	SI	12.2(2)T1	**28**
ROUTER	CISCO 1721	3	12.3(4)T4	SI	12.2(8)T4	**30**
ROUTER	CISCO 1711	3	12.2(15)ZL	SI	12.2(15)ZL	**167**
ROUTER	D-LINK DIR 600	3	1.04	SI	1.04	**45**
RADIO	ALVARION BREEZE ACCES VL 5.8	2		N/A	N/A	**2**
RADIO	UBIQUITI NANO BRIDGE M5	3	5.1.2	SI	5.6.1	**388**
RADIO	UBIQUITI *BULLET* M5	3	5.5	SI	5.6.1	**60**
RADIO	UBIQUITI NANO STATION 5	3	4.0.4	NO	N/A	**54**
RADIO	UBIQUITI POWER STATION 5	3	4.0.4	NO	N/A	**36**

Todos los *routers* indicados en la Tabla 3.3 soportan IPv6 en Doble Pila. Los equipos de radio de capa 3 de la marca Ubiquiti Networks soportan IPv6 en la serie M5. Se requiere cambiar de equipos de la serie Ubiquiti Networks de la serie Station 5. Los radios Alvarion son equipos de capa 2 y por lo tanto son independientes del protocolo IP que transporten.

Se ha pensado en este segmento de red, utilizar equipos de radio capa 3 para el soporte IPv6, para ello, se deberá buscar la mejor opción de equipos de radio para reemplazar los que no funcionan en IPv6.

3.2 CONEXIÓN CON EL PROVEEDOR IPv6 Y ANCHO DE BANDA REQUERIDO

En el Ecuador, la adopción del nuevo protocolo no está difundido o no tiene un despliegue considerable, sin embargo, el Ministerio de Telecomunicaciones y la Sociedad de la Información [19] trabajan en el diseño de políticas y mecanismos técnicos para una transición adecuada y ordenada por parte de los operadores, ISP, organismos del sector público y privado, etc.

El número de bloques IPv6 asignados y utilizados [20] en el Ecuador ha crecido muy poco en los últimos años. La cantidad de prefijos son:

- 51 bloques IPv6 asignados/distribuidos por LACNIC [21] a organizaciones ecuatorianas.
- 36 bloques utilizados (vistos en el Internet Global).
- 18 organizaciones diferentes utilizan prefijos IPv6.

La adopción del nuevo protocolo va de la mano de la oferta de servicios con soporte de IPv6 que se ofrecen actualmente en el Ecuador. Los servicios son los siguientes:

- El punto de intercambio de tráfico local de Internet (NAP.EC) tiene IPv6 nativo habilitado.

- Proveedores (ISP) que pueden proveer tránsito IPv6 nativo: 4. Ver Tabla 3.4. [22].

- Proveedores (ISP) que proveen servicio *home* con soporte IPv6 nativo: 0

Todos los proveedores que tienen soporte nativo IPv6 en Ecuador, promocionan sus servicios del nuevo protocolo de Internet únicamente vía telefónica, ya que al no ofrecer directamente el servicio de Internet IPv6 a clientes finales, mantienen en *stand by* la publicación del servicio IPv6 en su *web*.

Tabla 3.4 Proveedores IPv6 Ecuador

ASN	Nombre	Adyacencias IPv6	Rutas IPv6
AS27757	CORPORACIÓN NACIONAL DE TELECOMUNICACIONES - CNT EP	6	80
AS19169	Telconet S.A	6	13
AS23487	CONECEL	3	10
AS22724	PUNTONET S.A.	5	9
AS27814	Aeprovi	4	6
AS14522	Satnet	3	6
AS27765	TRANSNEXA S.A. E.M.A.	3	5
AS19114	Otecel S.A.	3	4

De los tres proveedores consultados para brindar la salida internacional en IPv6 se escogió a CNT EP como posible proveedor IP4/IPv6 ya que manejan costos más bajos, por tratarse de una empresa pública, que el resto de empresas competidoras. CNT EP garantiza un 99,8% de disponibilidad del servicio.

El costo del servicio que ofrece CNT EP, en Doble Pila, está directamente relacionado con la cantidad de ancho de banda demandada para cubrir las necesidades en las 5 ciudades en estudio (Quito, Cayambe, Latacunga, Otavalo, Ibarra).

El nuevo tráfico IPv6 que proporcionará la red, no aumentará el ancho de banda que demandaba un usuario, ya que se puede decir que el tráfico IPv6 se “roba” del tráfico IPv4. Lo único que aumentará son los recursos que demandará cada equipo ya que trabajarán con 2 protocolos en paralelo.

La habilitación del servicio IPv6 por parte del proveedor es muy simple. Lo que se debe realizar es levantar una sesión BGP en el *router* de borde para poder anunciar los prefijos tanto de Ecuaonline S.A como los prefijos que anuncia el proveedor.

El prefijo más pequeño para poder publicar por BGP es un /48 y el más grande en Ecuador es un /30. Las configuraciones de los equipos se verán más adelante.

3.3 PROCEDIMIENTO PARA LA ADQUISICIÓN DE UN *POOL* DE DIRECCIONES IPV6

La distribución y asignación de direcciones IPv6 para la región de América Latina y el Caribe está bajo la administración de LACNIC, entidad encargada de brindar el servicio de registro y asignación de direcciones IP y ASN para las organizaciones de la región.

Los recursos de Internet que pueden ser solicitados directamente a LACNIC son:

- ASN (*Autonomous System Number*).
- Bloque de direcciones IPv4 para Proveedores (agotado).
- Bloque de direcciones IPv4 para usuarios finales (agotado).
- Bloque de direcciones IPv6 para Proveedores.
- Bloque de direcciones IPv6 para usuarios finales.

Para solicitar cualquiera de estos recursos, se debe llenar un formulario y enviarlo por *e-mail* a la dirección hostmaster@lacnic.net. Una vez verificado el formulario sin encontrar ningún error, se generará un número de "*ticket*" que identifica la solicitud.

Una vez aprobada la solicitud de asignación inicial, se enviará un *e-mail* con información sobre el pago y sobre el acuerdo que debe ser firmado. La asignación solamente será hecha después de la recepción del pago y del acuerdo firmado.

Para ingresar la solicitud de manera exitosa se deben seguir los siguientes pasos.

1. Acceso al sistema de solicitud de recursos de LACNIC con el respectivo usuario y contraseña de la organización interesada en la obtención del prefijo IPv6, tal como se muestra en la Figura 3.1.

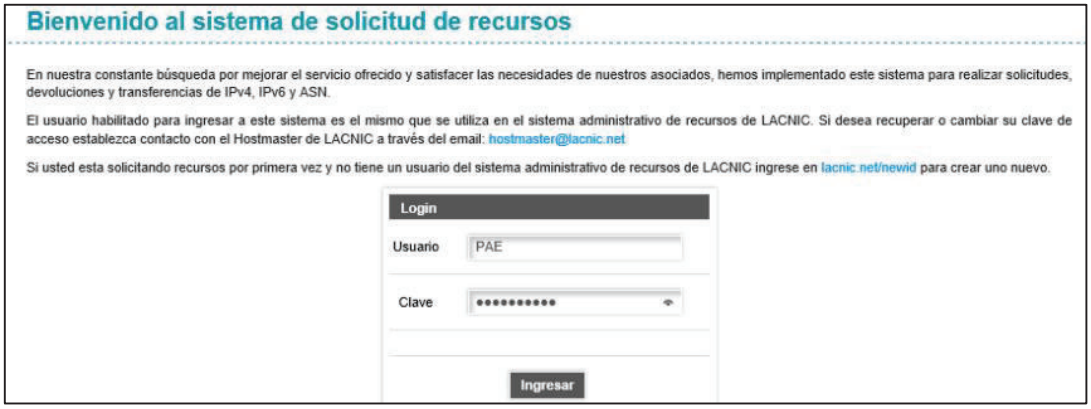


Figura 3.1 Acceso al sistema de LACNIC

2. Seleccionar la organización para la cual el *user-ID* es contacto administrativo, tal como se muestra en la Figura 3.2.

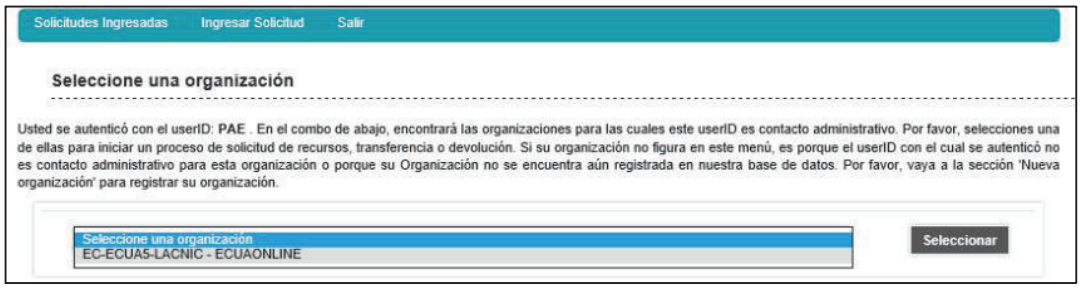


Figura 3.2 Selección de la organización

3. Selección del tipo de solicitud que desea ingresar la organización, ver Figura 3.3. Entre los distintos tipos es posible elegir una de las siguientes opciones:

- Solicitud de Número de sistemas Autónomos – (ASN).
- Solicitud IP versión 4 (IPv4 – Para ISP).
- Solicitud IP versión 6 (IPv6 – Para ISP).
- Solicitud de devolución de ASN, IPv4 y/o IPv6.
- Solicitud de transferencia de ASN, IPv4 y/o IPv6.

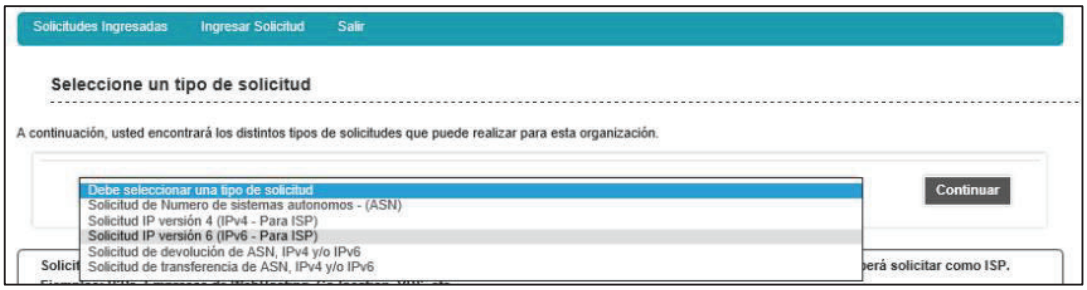


Figura 3.3 Selección del tipo de solicitud

4. Ingreso de la solicitud con los datos correctos y prestar atención en llenar los campos obligatorios. Cabe aclarar que los datos ingresados deben ser verídicos y con una descripción breve de lo que se requiere, entre estos datos se debe indicar el *pool* que se desea obtener, la fecha estimada de despliegue de la red IPv6, el plan de utilización y el plan de asignación de direcciones, entre otros, tal como se muestra en la Figura 3.4.

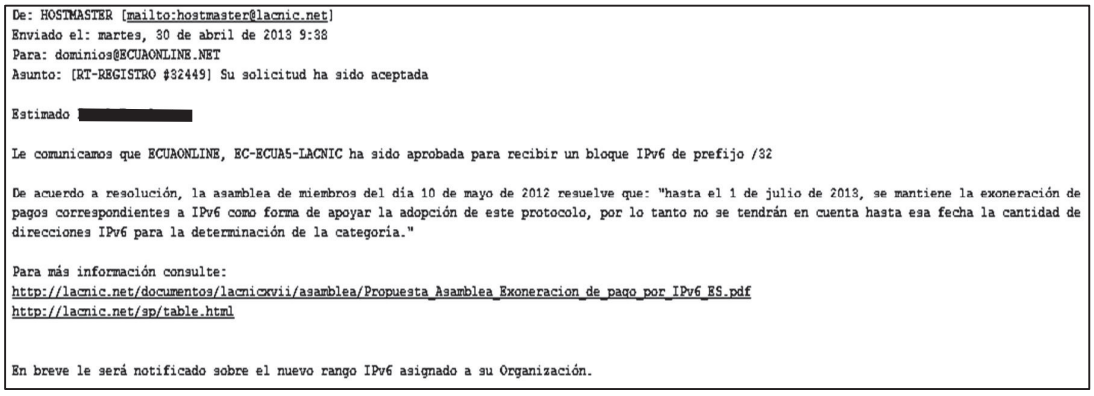
El bloque mínimo asignado por LACNIC es un /32 y para calificar para la asignación inicial, la organización debe:

- Ser un LIR (*Local Internet Registry*), o sea, una organización que asigna direcciones para usuarios de los servicios de red que provee; en general corresponde a los proveedores de acceso (ISP), cuyos clientes son los usuarios finales u otros proveedores de acceso.
- No ser un sitio final (usuario final).

- Documentar un plan detallado sobre los servicios y la conectividad en IPv6 a ofrecer a otras organizaciones (clientes).

Figura 3.4 Solicitud IP versión 6 (IPv6 - Para ISP)

La solicitud para obtener el prefijo IPv6 fue enviada el 25 de abril de 2013 y como resultado se recibió 5 días después la respuesta de aprobación, tal como lo indica la Figura 3.5.


De: HOSTMASTER [mailto:hostmaster@lacnic.net]
Enviado el: martes, 30 de abril de 2013 9:38
Para: dominios@ECUAONLINE.NET
Asunto: [RT-REGISTRO #32449] Su solicitud ha sido aceptada

Estimado [redacted]

Le comunicamos que ECUAONLINE, EC-ECUA5-LACNIC ha sido aprobada para recibir un bloque IPv6 de prefijo /32

De acuerdo a resolución, la asamblea de miembros del día 10 de mayo de 2012 resuelve que: "hasta el 1 de julio de 2013, se mantiene la exoneración de pagos correspondientes a IPv6 como forma de apoyar la adopción de este protocolo, por lo tanto no se tendrán en cuenta hasta esa fecha la cantidad de direcciones IPv6 para la determinación de la categoría."

Para más información consulte:
http://lacnic.net/documentos/lacnicxvii/asamblea/Propuesta_Asamblea_Exoneracion_de_pago_por_IPv6_ES.pdf
http://lacnic.net/sp/table.html

En breve le será notificado sobre el nuevo rango IPv6 asignado a su Organización.

Figura 3.5 Correo de aceptación de la solicitud de bloque IPv6

El bloque IPv6 que fue asignado a Ecuaonline S.A como resultado del proceso realizado fue el **2803:0b00::/32.**

3.4 DIRECCIONAMIENTO IPv6

Para seleccionar el mejor plan de direccionamiento hay que tomar en cuenta la agrupación de los rangos de direcciones en forma lógica y eficaz con el fin de obtener ventajas como:

- Facilidad de implementación de políticas de seguridad: como las ACL[13] o reglas de los *firewalls*.
- Trazabilidad de las direcciones: dentro de las propias direcciones, que se pueda descubrir información como localización, tipo y/o uso.
- Escalabilidad: a medida que una organización crezca. El plan de direccionamiento permitirá ese crecimiento de forma lógica.
- Una gestión de red más eficiente.

Las direcciones IPv6 se agrupan mediante el valor binario de la dirección. Este agrupamiento se lleva a cabo con los prefijos. Los prefijos representan a todas aquellas direcciones que empiezan con la misma serie de bits, y hasta determinada longitud representada por un "/NN".

Por ejemplo, el prefijo: 2803:b00::/32 contiene todas las direcciones que comienzan en 2803:b00:0:0:0:0:0:0 y terminan en 2803:b00:ffff:ffff:ffff:ffff:ffff:ffff.

Es decir, los 32 primeros bits son fijos (representado hexadecimalmente como "2803:b00"), y el resto varía. Puesto que cada dígito hexadecimal agrupa 4 bits, es muy recomendable el usar prefijos cuya longitud sea múltiplo de 4, como por ejemplo /48->/52->/56->/60->64.

[13] Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición.

Como se puede ver en la Figura 3.6, los prefijos con longitud múltiplo de 4 permiten localizar fácilmente su último dígito hexadecimal dentro de la dirección IPv6:

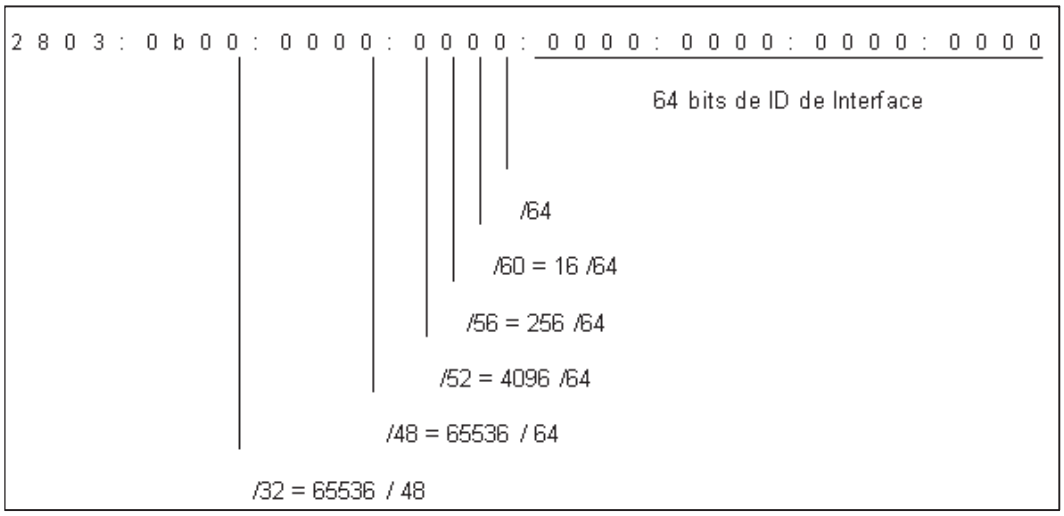


Figura 3.6 Prefijos con longitud múltiplo de 4

De acuerdo al estándar RFC 3177 de los prefijos dentro de una red, la asignación recomendada se la debe gestionar de la siguiente manera:

- Asignar /32 a ISP o LIRs (*Local Internet Registry*) con lo cual el número de direcciones disponibles sería 2^{96}.
- Asignar /48, para el caso general (Organización), excepto para los subscriptores muy grandes, con lo cual el número de direcciones disponibles sería 2^{80}.
- Asignar /64, cuando solo se tendrá una sola red en el diseño, es decir, para una red de alguna organización con lo cual se tendrían 2^{64} direcciones disponibles.
- Asignar /128, cuando solo existe un único *host* conectado (PC, servidor, Impresora, *router*).

Para el direccionamiento de la red a diseñar se utilizará como ya se indicó, la dirección IPv6 *unicast*: **2803:b00::/32** que fue la que LACNIC entregó al proveedor Ecuaonline.

La dirección *unicast* para la red IPv6 en hexadecimal es: 2803:b00::/32 y en notación binaria es: 0010 1000 0000 0011 0000 1011 0000 0000, tal como se muestra en la Figura 3.7.

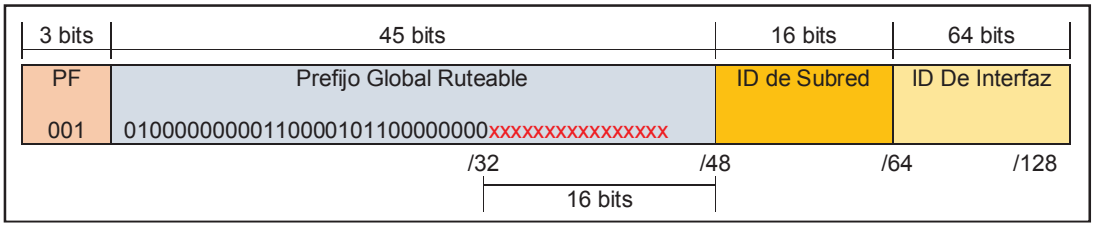


Figura 3.7 Dirección *unicast* 2803:0b00::/32

El direccionamiento será desarrollado analizando las regiones a las cuales el proveedor Ecuaonline S.A. brindará el servicio de Internet.

Considerando lo expuesto, y con la mentalidad de no abusar de la abundancia de direcciones IPv6, se plantea la asignación de la siguiente manera:

- DMZ (cuarto de servidores): Asignar un /64.
- VLAN: asignar un /64.
- Clientes considerados "*business"* (Empresas sin sucursales): Asignar un /52 a cada uno para el servicio de Internet contratado.
- Clientes considerados "*business* + Datos" (Empresas con sucursales): Asignar un /48 a cada uno para el servicio de Internet + Datos.
- Clientes "ISP" pequeños: Asignar un /40 a cada uno.
- Clientes "*home"* (Usuario doméstico): Asignar un /56 a cada uno.

Considerando esta asignación, se realizará el direccionamiento tomando en cuenta la información de las Tablas 2.6 a 2.10.

- # de DMZ: **1.**
- # VLAN: **5.**
    - VLAN 1: Gerencia – 2 usuarios.
    - VLAN 2: Ventas – 2 usuarios.
    - VLAN 3: Contabilidad – 3 usuarios.
    - VLAN 4: Desarrollo – 3 usuarios.
    - VLAN 5: Monitoreo – 5 Usuarios.
- Usuarios *business* + Datos en las 5 provincias: **26** empresas (Cada una puede tener 1, 2, 3 o 4 sucursales).
- Usuario *business*: **148** Empresas.
- Usuario ISP: **1** (Brighcell).
- Usuario *HOME*: **45** usuarios.

La información consolidada se la puede ver en la Tabla 3.5.

Tabla 3.5 Cantidad de usuarios en Quito, Latacunga, Otavalo, Cayambe e Ibarra

Provincia	*HOME*	*BUSINESS*	*BUSINESS* + Datos	ISP	VLAN	DMZ
QUITO	19	74	18	1	5	1
LATACUNGA	13	33	3	0	0	0
IBARRA	7	10	4	0	0	0
OTAVALO	2	4	1	0	0	0
CAYAMBE	4	27	0	0	0	0
TOTAL	**45**	**148**	**26**	**1**	**5**	**1**

Con esta información se puede ya realizar el direccionamiento dividido por grupos.

3.4.1 DIRECCIONAMIENTO INTRANET

La intranet en Ecuaonline S.A. está compuesta por 5 VLAN + 1 DMZ lo que suma un valor de 6 subredes a considerar. En total se empezará el diseño considerando que hay, hoy por hoy, 6 subredes.

- Asignación a cada Subred: prefijo /64.
- Número de redes necesarias: 6 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 3 bits.

Recordar

- $2^2=4$
- $2^3=8$
- $2^4=16$

Para las VLAN y DMZ se requieren 6 prefijos /64, es decir, se requieren como mínimo 3 bits de forma que 64 – 3 da un prefijo /61 que permite obtener hasta 8 prefijos /64.

Tabla 3.6 Detalles del prefijo IPv6 2803:0B00:0000:0000::/60

IP address	2803:b00::/60
TYPE	GLOBAL-*UNICAST*
NETWORK	2803:b00::
PREFIX LENGTH	60
NETWORK RANGE	2803:0b00:0000:0000:0000:0000:0000:0000- 2803:0b00:0000:000f:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	295147905179352825856
IP ADDRESS (FULL)	2803:0b00:0000:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Esta asignación es muy apretada ya que en un futuro la red no podrá aumentar en más de 8 subredes. Para resolver esto, se decide dar un prefijo /60 para cubrir a futuro 16 subredes /64.

El prefijo asignado a la intranet es el 2803:0B00:0000:0000::/60 y los detalles se los presenta en la Tabla 3.6 y las direcciones IP disponibles están en la Tabla 3.7. Para revisar el rango completo de direcciones ver la Tabla B-1 del Anexo B.

Tabla 3.7 Rango de direcciones IPv6 disponibles para las subredes de la Intranet

#	*Networks (on nibble-boundary) (16 total)*	*IPv6.arpa addresses*
1	2803:0b00:0000:0000:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0000:0001:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
16	2803:0b00:0000:000f:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.0.0.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.2 DIRECCIONAMIENTO USUARIOS *BUSINESS* + DATOS

La red de usuarios *business* + Datos de Ecuaonline S.A. está compuesta por 26 usuarios, es decir, se requieren de 26 subredes.

- Asignación a cada Subred: prefijo /48.
- Número de redes necesarias: 26 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 5 bits.

Recordar:

- 2^4=16
- 2^5=32
- 2^6=64

Para los usuarios *business* + Datos se requieren de 26 prefijos /48, es decir, se requieren como mínimo 5 bits de forma que 48 – 5 da un prefijo /43 que permite obtener hasta 32 prefijos /48.

Esta asignación es muy apretada ya que en un futuro la red no podrá aumentar en más de 32 subredes. Para resolver esto, se decide dar un prefijo /42 para cubrir a futuro 64 subredes /48.

El prefijo asignado a los usuarios *business* + Datos es el 2803:0B00:0040::/42 y los detalles se los presenta en la Tabla 3.8 y las direcciones IP disponibles están en la Tabla 3.9. Para revisar el rango completo de direcciones ver la Tabla B-2 del Anexo B.

Tabla 3.8 Detalle del prefijo IPv6 2803:0B00:0040::/42

IP *address*	2803:b00:40::/42
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:40::
PREFIX LENGTH	42
NETWORK RANGE	2803:0b00:0040:0000:0000:0000:0000:0000- 2803:0b00:007f:ffff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	77371252455336267181195264
IP ADDRESS (FULL)	2803:0b00:0040:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Tabla 3.9 Rango de direcciones IPv6 disponibles para los usuarios *business* + Datos

#	*Networks (on nibble-boundary) (64 total)*	*IPv6.arpa addresses*
1	2803:0b00:0040:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0041:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
64	2803:0b00:007f:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.3 DIRECCIONAMIENTO USUARIOS QUITO

En la ciudad de Quito se tienen 3 tipos de usuarios:

- Usuarios *business.*
- Usuarios *home.*
- Usuarios ISP.

3.4.3.1 Direccionamiento Usuarios *Business* de Quito

La red de usuarios *business* de la ciudad de Quito está compuesta por 74 usuarios, es decir, se requieren de 74 subredes.

- Asignación a cada Subred: prefijo /52.
- Número de redes necesarias: 74 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 7 bits.

Recordar

- $2^6=64$
- $2^7=128$
- $2^8=256$

Para los usuarios *business* de la ciudad de Quito se requieren de 74 prefijos /52, es decir, se requieren como mínimo 7 bits de forma que 52 – 7 da un prefijo /45 que permite obtener hasta 128 prefijos /52.

El prefijo asignado a los usuarios *Business* de la ciudad de Quito es el 2803:0B00:05F8::/45 y los detalles se los presenta en la Tabla 3.10 y las direcciones IP disponibles están en la Tabla 3.11. Para revisar el rango completo de direcciones ver la Tabla B-3 del Anexo B.

Tabla 3.10 Detalle del prefijo IPv6 2803:0B00:05F8::/45

IP address	2803:b00:5f8::/45
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:5f8::
PREFIX LENGTH	45
NETWORK RANGE	2803:0b00:05f8:0000:0000:0000:0000:0000- 2803:0b00:05ff:ffff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	967140655691703339764940 8
IP ADDRESS (FULL)	2803:0b00:05f8:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa

Tabla 3.11 Rango de direcciones IPv6 disponibles para los usuarios *business* de Quito

#	*Networks (on nibble-boundary) (128 total)*	*IPv6.arpa addresses*
1	2803:0b00:05f8:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:05f8:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
128	2803:0b00:05ff:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.3.2 Direccionamiento Usuarios *Home* de Quito

La red de usuarios *Home* de la ciudad de Quito está compuesta por 19 usuarios, es decir, se requieren de 19 subredes.

- Asignación a cada Subred: prefijo /56.
- Número de redes necesarias: 19 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 5 bits.

Recordar:

- 2^4=16

- 2^5=32
- 2^6=64

Para los usuarios *home* de la ciudad de Quito se requieren de 19 prefijos /56, es decir, se requieren como mínimo 5 bits de forma que 56 – 5 da un prefijo /51 que permite obtener hasta 32 prefijos /56.

El prefijo asignado a los usuarios *home* de la ciudad de Quito es el 2803:0B00:0400:0000::/51 y los detalles se los presenta en la Tabla 3.12 y las direcciones IP disponibles están en la Tabla 3.13. Para revisar el rango completo de direcciones ver la Tabla B-4 del Anexo B.

Tabla 3.12 Detalle del prefijo IPv6 2803:0B00:0400:0000::/51

IP address	2803:b00:400::/51
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:400::
PREFIX LENGTH	51
NETWORK RANGE	2803:0b00:0400:0000:0000:0000:0000:0000- 2803:0b00:0400:1fff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	151115727451828646838272
IP ADDRESS (FULL)	2803:0b00:0400:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa

Tabla 3.13 Rango de direcciones IPv6 disponibles para los usuarios *home* de Quito

#	*Networks (on nibble-boundary) (32 total)*	*IPv6.arpa addresses*
1	2803:0b00:0400:0000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0400:0100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
32	2803:0b00:0400:1f00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.3.3 Direccionamiento Usuario ISP de Quito

El único usuario que es proveedor de servicios de Internet ISP en la ciudad de Quito es Brighcell del Ecuador [23].

- Asignación a cada Subred: prefijo /40.
- Número de redes necesarias: 1 subred.
- Bits necesarios para cubrir las necesidades de las subredes: 1 bit.

Recordar:

- $2^0=1$
- $2^1=2$
- $2^2=4$

Tabla 3.14 Detalle del prefijo IPv6 2803:0B00:0600::/39

IP address	2803:b00:600::/39
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:600::
PREFIX LENGTH	39
NETWORK RANGE	2803:0b00:0600:0000:0000:0000:0000:0000- 2803:0b00:07ff:ffff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	618970019642690137449562112
IP ADDRESS (FULL)	2803:0b00:0600:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.0.0.b.0.3.0.8.2.ip6.arpa

Para el ISP de la ciudad de Quito se requiere de 1 prefijo /40, es decir, se requieren como mínimo 1 bit de forma que 40 – 1 da un prefijo /39 que permite obtener hasta 2 prefijos /40.

El prefijo asignado al ISP de la ciudad de Quito es el 2803:0B00:0600::/39 y los detalles se los presenta en la Tabla 3.14 y las direcciones IP disponibles están en la Tabla 3.15.

Tabla 3.15 Rango de direcciones IPv6 disponibles para los clientes ISP de Quito

#	*Networks (on nibble-boundary) (2 total)*	*IPv6.arpa addresses*
1	2803:0b00:0600:0000:0000:0000:0000:0000/40	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0700:0000:0000:0000:0000:0000/40	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.4 DIRECCIONAMIENTO USUARIOS LATACUNGA

En la ciudad de Latacunga se tienen 2 tipos de usuarios:

- Usuarios *business.*
- Usuarios *home.*

3.4.4.1 Direccionamiento Usuarios *Business* de Latacunga

Los usuarios *business* de la ciudad de Latacunga está compuesta por 33 usuarios, es decir, se requieren de 33 subredes.

- Asignación a cada Subred: prefijo /52.
- Número de redes necesarias: 33 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 6 bits.

Recordar:

- $2^5=32$
- $2^6=64$
- $2^7=128$

Para los usuarios *business* de la ciudad de Latacunga se requieren de 33 prefijos /52, es decir, se requieren como mínimo 6 bits de forma que 52 – 6 da un prefijo /46 que permite obtener hasta 64 prefijos /52.

El prefijo asignado a los usuarios *business* de la ciudad de Latacunga es el 2803:0B00:001C::/46 y los detalles se los presenta en la Tabla 3.16 y las direcciones IP disponibles están en la Tabla 3.17. Para revisar el rango completo de direcciones ver la Tabla B-5 del Anexo B.

Tabla 3.16 Detalle del prefijo IPv6 2803:0B00:001C::/46

IP address	2803:b00:1c::/46
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:1c::
PREFIX LENGTH	46
NETWORK RANGE	2803:0b00:001c:0000:0000:0000:0000:0000- 2803:0b00:001f:ffff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	4835703278458516698824704
IP ADDRESS (FULL)	2803:0b00:001c:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Tabla 3.17 Rango de direcciones IPv6 disponibles para los usuarios *business* de Latacunga

#	*Networks (on nibble-boundary) (64 total)*	*IPv6.arpa addresses*
1	2803:0b00:001c:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:001c:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
64	2803:0b00:001f:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.4.2 Direccionamiento Usuarios *home* de Latacunga

Los usuarios *home* de la ciudad de Latacunga está compuesta por 13 usuarios, es decir, se requieren de 13 subredes.

- Asignación a cada Subred: prefijo /56.
- Número de redes necesarias: 13 subredes.

- Bits necesarios para cubrir las necesidades de las subredes: 4 bits.

Recordar:

- $2^3=8$
- $2^4=16$
- $2^5=32$

Para los usuarios *home* de la ciudad de Latacunga se requieren de 13 prefijos /56, es decir, se requieren como mínimo 4 bits de forma que 56 – 4 da un prefijo /52 que permite obtener hasta 16 prefijos /56.

Tabla 3.18 Detalle del prefijo IPv6 2803:0B00:0018:0000::/52

IP address	2803:b00:18::/52
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:18::
PREFIX LENGTH	52
NETWORK RANGE	2803:0b00:0018:0000:0000:0000:0000:0000- 2803:0b00:0018:0fff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	75557863725914323419136
IP ADDRESS (FULL)	2803:0b00:0018:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Tabla 3.19 Rango de direcciones IPv6 disponibles para los usuarios *home* de Latacunga

#	*Networks (on nibble-boundary) (16 total)*	*IPv6.arpa addresses*
1	2803:0b00:0018:0000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0018:0100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
16	2803:0b00:0018:0f00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

El prefijo asignado a los usuarios *home* de la ciudad de Latacunga es el 2803:0B00:0018:0000::/52 y los detalles se los presenta en la Tabla 3.18 y las direcciones IP disponibles están en la Tabla 3.19. Para revisar el rango completo de direcciones ver la Tabla B-6 del Anexo B.

3.4.5 DIRECCIONAMIENTO USUARIOS IBARRA

En la ciudad de Ibarra se tienen 2 tipos de usuarios:

- Usuarios *business.*
- Usuarios *home.*

3.4.5.1 Direccionamiento Usuarios *business* de Ibarra

Los usuarios *BUSINESS* de la ciudad de Ibarra está compuesta por 10 usuarios, es decir, se requieren de 10 subredes.

- Asignación a cada Subred: prefijo /52.
- Número de redes necesarias: 10 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 4 bits.

Recordar:

- $2^3=8$
- $2^4=16$
- $2^5=32$

Para los usuarios *business* de la ciudad de Ibarra se requieren de 10 prefijos /52, es decir, se requieren como mínimo 4 bits de forma que 52 – 4 da un prefijo /48 que permite obtener hasta 16 prefijos /52.

El prefijo asignado a los usuarios *business* de la ciudad de Ibarra es el 2803:0B00:0011::/48 y los detalles se los presenta en la Tabla 3.20 y las direcciones IP disponibles están en la Tabla 3.21. Para revisar el rango completo de direcciones ver la Tabla B-7 del Anexo B.

Tabla 3.20 Detalle del prefijo IPv6 2803:0B00:0011::/48

IP address	2803:b00:11::/48
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:11::
PREFIX LENGTH	48
NETWORK RANGE	2803:0b00:0011:0000:0000:0000:0000:0000- 2803:0b00:0011:ffff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	1208925819614629174706176
IP ADDRESS (FULL)	2803:0b00:0011:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Tabla 3.21 Rango de direcciones IPv6 disponibles para los usuarios *business* de Ibarra

#	*Networks (on nibble-boundary) (16 total)*	*IPv6.arpa addresses*
1	2803:0b00:0011:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0011:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
16	2803:0b00:0011:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.1.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.5.2 Direccionamiento Usuarios *home* de Ibarra

Los usuarios *home* de la ciudad de Ibarra está compuesta por 7 usuarios, es decir, se requieren de 7 subredes.

- Asignación a cada Subred: prefijo /56.
- Número de redes necesarias: 7 subredes.

- Bits necesarios para cubrir las necesidades de las subredes: 3 bits.

Recordar:

- $2^3=8$
- $2^4=16$
- $2^5=32$

Para los usuarios *home* de la ciudad de Ibarra se requieren de 7 prefijos /56, es decir, se requieren como mínimo 3 bits de forma que 56 – 3 da un prefijo /53 que permite obtener hasta 8 prefijos /56.

Tabla 3.22 Detalle del prefijo IPv6 2803:0B00:0010:0000::/52

IP address	2803:b00:10::/52
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:10::
PREFIX LENGTH	52
NETWORK RANGE	2803:0b00:0010:0000:0000:0000:0000:0000- 2803:0b00:0010:0fff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	75557863725914323419136
IP ADDRESS (FULL)	2803:0b00:0010:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Tabla 3.23 Rango de direcciones IPv6 disponibles para los usuarios *home* de Ibarra

#	*Networks (on nibble-boundary) (16 total)*	*IPv6.arpa addresses*
1	2803:0b00:0010:0000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0010:0100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
16	2803:0b00:0010:0f00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.0.0.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Esta asignación es muy apretada ya que en un futuro la red no podrá aumentar en más de 8 subredes. Para resolver esto, se decide dar un prefijo /52 para cubrir a futuro 16 subredes /56.

El prefijo asignado a los usuarios *home* de la ciudad de Ibarra es el 2803:0B00:0010:0000::/52 y los detalles se los presenta en la Tabla 3.22 y las direcciones IP disponibles están en la Tabla 3.23. Para revisar el rango completo de direcciones ver la Tabla B-8 del Anexo B.

3.4.6 DIRECCIONAMIENTO USUARIOS OTAVALO

En la ciudad de Otavalo se tienen 2 tipos de usuarios:

- Usuarios *business.*
- Usuarios *home.*

3.4.6.1 Direccionamiento Usuarios *business* de Otavalo

La red de usuarios *business* de la ciudad de Otavalo está compuesta por 4 usuarios, es decir, se requieren de 4 subredes.

- Asignación a cada Subred: prefijo /52.
- Número de redes necesarias: 4 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 2 bits.

Recordar:

- $2^1=2$
- $2^2=4$
- $2^3=8$

Para los usuarios *business* de la ciudad de Otavalo se requieren de 4 prefijos /52, es decir, se requieren como mínimo 2 bits de forma que 52 – 2 da un prefijo /50 que permite obtener hasta 4 prefijos /52.

Esta asignación es muy apretada ya que en un futuro la red no podrá aumentar en más de 4 subredes. Para resolver esto, se decide dar un prefijo /48 para cubrir a futuro 16 subredes /52.

El prefijo asignado a los usuarios *business* de la ciudad de Otavalo es el 2803:0B00:0013::/48 y los detalles se los presenta en la Tabla 3.24 y las direcciones IP disponibles están en la Tabla 3.25. Para revisar el rango completo de direcciones ver la Tabla B-9 del Anexo B.

Tabla 3.24 Detalle del prefijo IPv6 2803:0B00:0013::/48

IP address	2803:b00:13::/48
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:13::
PREFIX LENGTH	48
NETWORK RANGE	2803:0b00:0013:0000:0000:0000:0000:0000- 2803:0b00:0013:ffff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	1208925819614629174706176
IP ADDRESS (FULL)	2803:0b00:0013:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Tabla 3.25 Rango de direcciones IPv6 disponibles para los usuarios *business* de Otavalo

#	*Networks (on nibble-boundary) (16 total)*	*IPv6.arpa addresses*
1	2803:0b00:0013:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0013:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
16	2803:0b00:0013:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.6.2 Direccionamiento Usuarios *home* de Otavalo

La red de usuarios *home* de la ciudad de Otavalo está compuesta por 2 usuarios, es decir, se requieren de 2 subredes.

- Asignación a cada Subred: prefijo /56.
- Número de redes necesarias: 2 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 1 bits.

Recordar:

- $2^1=2$
- $2^2=4$
- $2^3=8$

Para los usuarios *home* de la ciudad de Otavalo se requieren de 2 prefijos /56, es decir, se requiere como mínimo 1 bit de forma que 56 – 1 da un prefijo /55 que permite obtener hasta 2 prefijos /56.

Esta asignación es muy apretada ya que en un futuro la red no podrá aumentar en más de 2 subredes. Para resolver esto, se decide dar un prefijo /54 para cubrir a futuro 4 subredes /56.

Tabla 3.26 Detalle del prefijo IPv6 2803:0B00:0012:0000::/54

IP address	2803:b00:12::/54
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:12::
PREFIX LENGTH	54
NETWORK RANGE	2803:0b00:0012:0000:0000:0000:0000:0000- 2803:0b00:0012:03ff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	18889465931478580854784
IP ADDRESS (FULL)	2803:0b00:0012:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

El prefijo asignado a los usuarios *home* de la ciudad de Otavalo es el 2803:0B00:0012:0000::/54 y los detalles se los presenta en la Tabla 3.26 y las direcciones IP disponibles están en la Tabla 3.27.

Tabla 3.27 Rango de direcciones IPv6 disponibles para los usuarios *home* de Otavalo

#	Networks (on nibble-boundary) (4 total)	IPv6.arpa addresses
1	2803:0b00:0012:0000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0012:0100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.2.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0012:0200:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.2.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0012:0300:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.2.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.7 DIRECCIONAMIENTO USUARIOS CAYAMBE

En la ciudad de Cayambe se tienen 2 tipos de usuarios:

- Usuarios *business.*
- Usuarios *home.*

3.4.7.1 Direccionamiento Usuarios *business* de Cayambe

La red de usuarios *business* de la ciudad de Cayambe está compuesta por 27 usuarios, es decir, se requieren de 27 subredes.

- Asignación a cada Subred: prefijo /52.
- Número de redes necesarias: 27 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 5 bits.

Recordar:

- 2^4=16
- 2^5=32
- 2^6=64

Para los usuarios *business* de la ciudad de Cayambe se requieren de 27 prefijos /52, es decir, se requieren como mínimo 5 bits de forma que 52 – 5 da un prefijo /47 que permite obtener hasta 32 prefijos /52.

Tabla 3.28 Detalle del prefijo IPv6 2803:0B00:0016::/47

IP address	2803:b00:16::/47
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:16::
PREFIX LENGTH	47
NETWORK RANGE	2803:0b00:0016:0000:0000:0000:0000:0000- 2803:0b00:0017:ffff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	241785163922925834941235 2
IP ADDRESS (FULL)	2803:0b00:0016:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Tabla 3.29 Rango de direcciones IPv6 disponibles para los usuarios *business* de Cayambe

#	*Networks (on nibble-boundary) (32 total)*	*IPv6.arpa addresses*
1	2803:0b00:0016:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0016:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.6.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
32	2803:0b00:0017:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.7.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

El prefijo asignado a los usuarios *business* de la ciudad de Cayambe es el 2803:0B00:0016::/47 y los detalles se los presenta en la Tabla 3.28 y las

direcciones IP disponibles están en la Tabla 3.29. Para revisar el rango completo de direcciones ver la Tabla B-10 del Anexo B.

3.4.7.2 Direccionamiento Usuarios *home* de Cayambe

La red de usuarios *home* de la ciudad de Cayambe está compuesta por 4 usuarios, es decir, se requieren de 4 subredes.

- Asignación a cada Subred: prefijo /56.
- Número de redes necesarias: 4 subredes.
- Bits necesarios para cubrir las necesidades de las subredes: 2 bits.

Recordar

- $2^1=2$
- $2^2=4$
- $2^3=8$

Para los usuarios *home* de la ciudad de Cayambe se requieren de 4 prefijos /56, es decir, se requieren como mínimo 2 bits de forma que 56 – 2 da un prefijo /54 que permite obtener hasta 4 prefijos /56.

Tabla 3.30 Detalle del prefijo IPv6 2803:0B00:0014:0000::/53

IP address	2803:b00:14::/53
TYPE	*GLOBAL-UNICAST*
NETWORK	2803:b00:14::
PREFIX LENGTH	53
NETWORK RANGE	2803:0b00:0014:0000:0000:0000:0000:0000- 2803:0b00:0014:07ff:ffff:ffff:ffff:ffff
TOTAL IP ADDRESSES	3777893186295716170956 8
IP ADDRESS (FULL)	2803:0b00:0014:0000:0000:0000:0000:0000
IP6.ARPA FORMAT	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

Esta asignación es muy apretada ya que en un futuro la red no podrá aumentar en más de 4 subredes. Para resolver esto, se decide dar un prefijo /53 para cubrir a futuro 8 subredes /56.

El prefijo asignado a los usuarios *home* de la ciudad de Cayambe es el 2803:0B00:0014:0000::/53 y los detalles se los presenta en la Tabla 3.30 y las direcciones IP disponibles están en la Tabla 3.31. Para revisar el rango completo de direcciones ver la Tabla B-11 del Anexo B.

Tabla 3.31 Rango de direcciones IPv6 disponibles para los usuarios *home* de Cayambe

#	Networks (on nibble-boundary) (8 total)	IPv6.arpa addresses
1	2803:0b00:0014:0000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0014:0100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.4.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
⋮	⋮	⋮
8	2803:0b00:0014:0700:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.4.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

3.4.8 RESUMEN DE PREFIJOS NECESARIOS

Como resultado de los prefijos obtenidos y necesarios para cada usuario de cada provincia se requiere calcular el prefijo mínimo que requeriría Ecuaonline S.A. solicitar a LACNIC para cubrir la demanda de direccionamiento en estas ciudades.

Tabla 3.32 Cálculo para encontrar el prefijo mínimo para cubrir las necesidades

Prefijos Requeridos	/60+/54+/53+/52+/52+/51+/48+/48+/47+/46+/45+/43+/39
Prefijos descompuestos en el prefijo de referencia /60	1+64+128+256+256+512+4096+8192+16384+32768+131072+2097152
Suma de Prefijos /60	2294977
Prefijo requerido	/38

Para calcular el prefijo mínimo, que Ecuaonline S.A. debe utilizar para satisfacer las necesidades de las 5 provincias, se debe descomponer cada uno de los prefijos en un prefijo de referencia. Para calcular se escoge el prefijo de referencia /60 y se sumarizan todos los prefijos en base al prefijo de referencia, por ejemplo: el prefijo /54 tiene 64 prefijos /60. El cálculo para encontrar el prefijo mínimo se presenta en la Tabla 3.32:

Recordar

- 2^{21}= 2.097.152
- 2^{22}= 4.194.304
- 2^{23}= 8.388.608

En la Tabla 3.32 se indica que la cantidad de prefijos /60 suman 2.294.977, por lo tanto, se necesitan como mínimo 22 bits de forma que 60 – 22 da un prefijo /38.

En la siguiente Figura 3.8 se presenta la distribución de direcciones IPv6 con el prefijo que fue asignado por LACNIC a Ecuaonline S.A.

3.5 MECANISMOS DE TRANSICIÓN A ESCOGER

Como ya se revisó en el primer capítulo, el objetivo de una transición de IPv4 a IPv6 es buscar la manera de tener IPv6 en etapas dentro de una red.

De manera general, se buscará implementar como primera opción, Doble Pila o *Dual Stack*, ya que es una solución permanente y no requiere de cambios futuros en la red. Cuando no sea posible implementar *Dual Stack* en algún segmento de la red, se pensará en utilizar otros mecanismos de transición como los basados en túneles, pero siempre evitando al máximo utilizar este mecanismo, ya que no es una solución permanente y a futuro se necesitará hacer cambios en la red para tener una conexión IPv6 nativa.

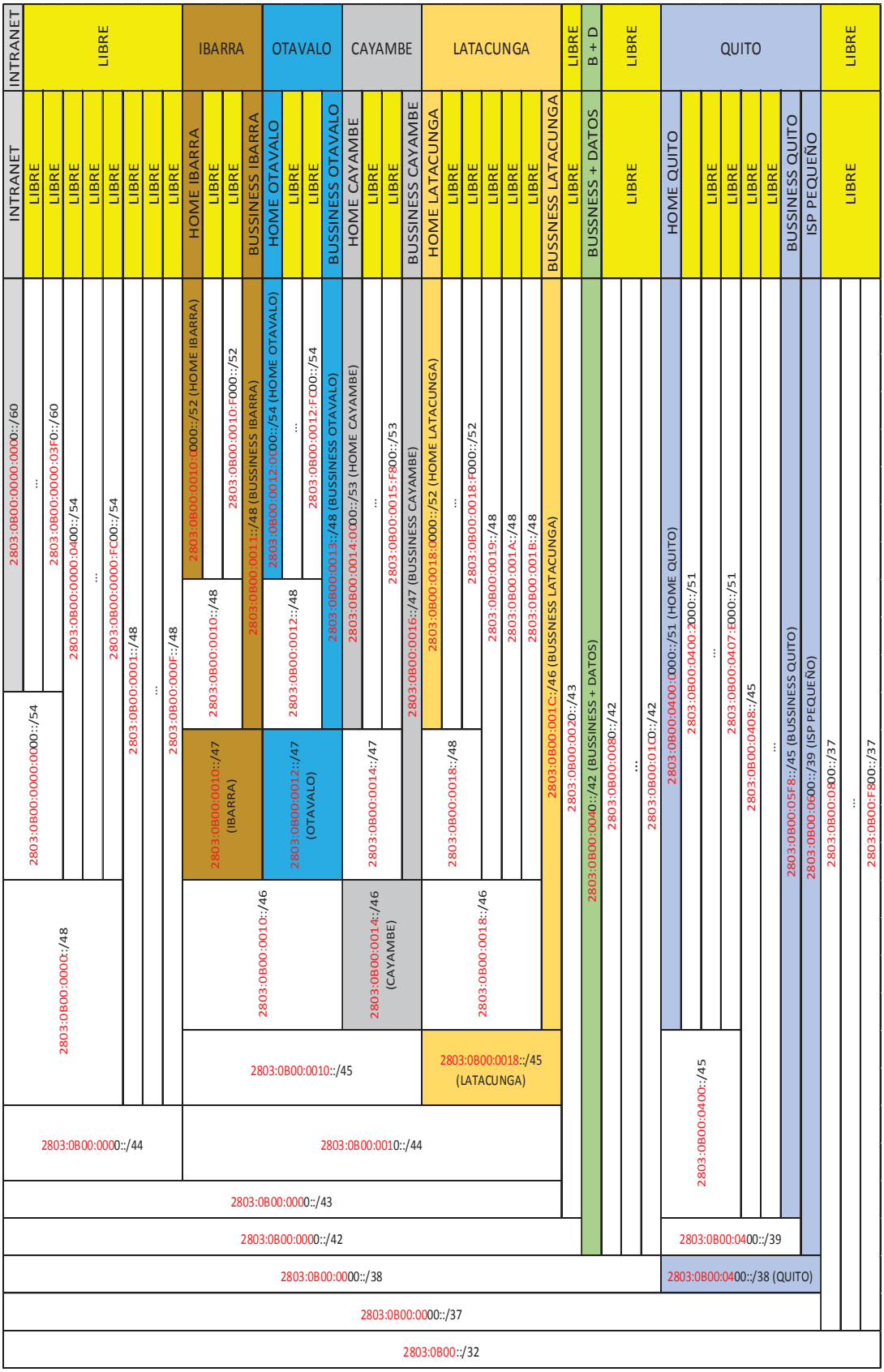


Figura 3.8: Distribución de direcciones IPv6

Considerando lo expuesto, es necesario conocer, si tanto los equipos, como los servicios de la red funcionarán en un futuro en IPv6 y además, se debe investigar si los equipos funcionarán en Doble Pila.

El orden en el cual se debe realizar la transición va desde el *Core* como primer segmento a ser tratado, después se continúa con la red de Distribución y finalmente se concluye con la red de Acceso hasta llegar donde el cliente

3.5.1 MECANISMO DE TRANSICIÓN EN LA RED DE *CORE*

Como parte del diseño de la red, se plantea utilizar Doble Pila en la red de *Core* y para ello, se necesitarán hacer algunos cambios en las configuraciones de los equipos que la componen. Los equipos en Doble Pila trabajarán con los dos protocolos de red al mismo tiempo, lo que demandará un aumento en el uso de los recursos de los equipos.

Para que el *Core* funcione en Doble Pila se analizará si los equipos que componen este segmento de red, soportan *dual stack*. (Ver Tabla 3.34).

Según lo que muestra la Tabla 3.33, la red de *Core* puede soportar *Dual Stack* al 86% (19 de los 22 equipos soportan Doble Pila) y el único limitante para que funcione al 100% es reemplazar los 3 equipos NetEnforcer AC-402 que no tienen soporte en el modelo que se usa actualmente.

Tabla 3.33 Soporte de equipos *Dual Stack* en la Red de *Core*

CORE			
EQUIPO	**MODELO**	**SOPORTA DUAL STACK**	**CANTIDAD**
ROUTER	CISCO 2921/K9	SI	**2**
SWITCH	CISCO WS-C3750G-24T	SI	**2**
NETENFORCER	AC-402	NO	**3**
CLON	*CORE* I5	SI	**13**
SERVER	HP-DL360P	SI	**1**
SERVER	CENTOS	SI	**1**

Para habilitar Doble Pila en una interfaz de cualquiera de los *routers* o *switches* de Cisco es necesario colocar los siguientes comandos.

- ***Router0>****enable*
- ***Router0#****configure terminal*
- *Enter configuration commands, one per line. End with CNTL/Z.*
- ***Router0(config)#****IPv6 unicast-routing -> habilita enrutamiento IPv6*
- ***Router0(config)#****interface S0/0/0*
- ***Router0(config-if)#****IPv6 enable -> Habilita el protocolo IPv6*
- ***Router0(config-if)#****ip address "prefijo_IPv4" "Mascara" -> configure IPv4 en la interfaz*
- ***Router0(config-if)#****IPv6 address "prefijo_IPv6" -> Configura IPv6 en la interfaz*
- ***Router0(config-if)#****clock rate 64000*
- ***Router0(config-if)#****no shutdown -> levanta la interfaz*
- *%LINK-5-CHANGED: Interface Serial0/0/0, changed state to down*

3.5.2 MECANISMO DE TRANSICIÓN EN LA RED DE DISTRIBUCIÓN

La red de Distribución está conformada en su totalidad por equipos de radio, capa 1 y capa 2 (22 radios, Ver Tabla 3.34), así como también de *switches* capa 2 para manejo de VLAN dentro de cada nodo. Por lo tanto, en este segmento de red, se requiere únicamente que el transporte entre nodos sea eficiente y estable. En este caso se tienen 3 escenarios posibles:

1. Utilizar la red de Distribución como se encuentra actualmente: con esta opción, el transporte de los datos se realizará de forma transparente a los protocolos de capas superiores.

2. Realizar un cambio completo a nuevos equipos WiFi que soporten IPv6.

3. Realizar un cambio completo de tecnología; es decir, se puede utilizar MPLS para toda la red de distribución, el desarrollo de esta alternativa está fuera de los alcances del presente proyecto.

Tabla 3.34 Soporte de equipos *Dual Stack* en la Red de Distribución

DISTRIBUCIÓN			
EQUIPO	**MODELO**	**SOPORTE IPv6**	**CANTIDAD**
RADIO	AIRMUX 400	N/A	**4**
RADIO	AIRMUX 200	N/A	**10**
ROUTER	D-LINK DIR 100	N/A	**22**
SWITCH	WS-C2960-24TT-L	N/A	**22**
RADIO	TELETRONICS TT 5800	N/A	**8**

Si se decide cambiar los equipos de radio para tener una red 100% IPv6, se debe verificar en el mercado las marcas que los proveedores ofrecen, entre ellas, se presentan en la Tabla 3.35 las más conocidas.

Si se elige la opción de dejar la red como está, no se requiere elegir un mecanismo de transición a implementar en este segmento de la red, ya que el transporte de IPv4 o IPv6 es totalmente independiente al trabajar con equipos de capa 1 o capa 2.

Tabla 3.35 Características de Radios

MARCA	EQUIPO	BANDA DE FRECUENCIA [GHz]	THROUGHPUT [Mbps]	ALCANCE [Km]
MIKROTIK	SXT5HPND	5.875GHz	550 Mbps	60 Km
ALTAI SUPER WIFI	A2e	5.15-5.35, 5.47-5.725, 5.725-5.825 GHz	450 Mbps	50 km
UBIQUITI	Rocket Titanium M5	5.1-5.8GHz	500 Mbps	70 km

Si se decide cambiar los equipos de radio por nuevos equipos con soporte IPv6, se debe entender que este segmento de red trabajará en Doble Pila.

La opción 3 está fuera del alcance de este proyecto, sin embargo, es citada para indicar que es posible utilizar otra tecnología que permita trasportar IPv6.

3.5.3 MECANISMO DE TRANSICIÓN EN LA RED DE ACCESO

La red de Acceso está conformada por *routers*, CPE de abonado, y radios para la parte de acceso.

Según la Tabla 3.36, todos los *routers* tienen soporte *Dual Stack*, mientras que del total de equipos de radio (540) solamente el 82,96% soportan Doble Pila. Los equipos que no soportan el nuevo protocolo IP (92 equipos) deben ser sustituidos para tener una conexión IPv6 nativa en este segmento de red.

Tabla 3.36 Soporte de equipos *Dual Stack* en la Red de Acceso

ACCESO				
EQUIPO	**MODELO**	**CAPA**	**SOPORTE IPv6**	**CANTIDAD**
ROUTER	CISCO 2610	3	SI	28
ROUTER	CISCO 1721	3	SI	30
ROUTER	CISCO 1711	3	SI	167
ROUTER	D-LINK DIR 600	3	SI	45
RADIO	ALVARION BREEZE ACCES VL 5.8	2	N/A	2
RADIO	UBIQUITI NANO BRIDGE M5	3	SI	388
RADIO	UBIQUITI *BULLET* M5	3	SI	60
RADIO	UBIQUITI NANO STATION 5	3	N/A	54
RADIO	UBIQUITI POWER STATION 5	3	N/A	36

3.6 SELECCIÓN DE EQUIPOS QUE SOPORTEN IPv6

Se debe considerar que para tener un soporte IPv6 nativo es necesario utilizar equipos que puedan trabajar en Doble Pila, para ello, se presentarán los equipos que se aconsejan utilizar, dentro de cada segmento de red, para tener una red 100% IPv6 nativa.

3.6.1 Equipos Nuevos para la Red de *Core*

Según el análisis anterior, se detectó que el equipo que no soporta IPv6 es el NetEnforcer AC-402 y por lo tanto requiere ser reemplazado.

Para reemplazar este equipo se pensó en comparar 2 marcas similares y que den las mismas funcionalidades. Las dos marcas a comparar son: NetEnforcer [24] y NetEcualizer [25].

Dentro de la marca NetEnforcer hay 4 versiones que soportan IPv6 en su totalidad:

- NETENFORCER AC-500
- NETENFORCER AC-1400
- NETENFORCER AC-3000
- NETENFORCER AC-6000

Tabla 3.37 Características de los modelos NetEnforcer

NETENFORCER				
CARACTERÍSTICAS	**AC 504**	**AC 1440**	**AC 3040**	**AC 6000**
Suscriptores	32.000	160.000	160.000	400.000
Bandwidth	200 Mpbs, full duplex	1 Gbps, full duplex	4 Gbps, full duplex	8 Gbps, full duplex
Puertos	4 x 10/100/1000 Mbps + 4 ports for cascading	8 x 1000BASE-SX/LX/ZX or 8 x 10/100/1000BASE-T (auto-negotiation)	8 x 1000BASE-SX/LX/ZX or 8 x 10/100/1000BASE-T (auto-negotiation)	10GE-BASE-SR/LR/ER, 1000BASE-SX/LX/ZX, and 100/1000BASE-T
IPv6	IPv4/IPv6 *Dual Stack* subscriber support for flexible network configuration	IPv4/IPv6 *Dual Stack* subscriber support for flexible network configuration	IPv4/IPv6 *Dual Stack* subscriber support for flexible network configuration	IPv4/IPv6 *Dual Stack* subscriber support for flexible network configuration
# Conexiones	400.000	3.500.000	3.500.000	10.000.000
Costo [26]	**$5.920,00**	**$20.600,00**	**$47.080,00**	**$49.720,00**

Dentro de la marca Netequalizer hay dos versiones que soportan IPv6:

- NETECUALIZER NE3000
- NETECUALIZER NE4000

En las Tablas 3.37 y 3.38 se pueden ver las características más relevantes de cada modelo.

De los modelos de los 2 fabricantes, y según las características que cada modelo posee, se recomienda adquirir 2 equipos NetEnforcer AC 504 para reemplazar los 3 equipos NetEnforcer 402.

Tabla 3.38 Características de los modelos *NetEcualizer*

NETECUALIZER		
CARACTERÍSTICAS	**NE3000**	**NE4000**
Suscriptores	20.000	40.000
Bandwidth	1 Gbps, *full duplex*	5 Gbps, full duplex
Puertos	2 - *copper* 10/100/1000 10 *Gbps copper optional* *Fiber optional*: 1Gbps & 10Gbps SM or MM	2 - *copper* 10/100/1000 10 Gbps *copper optional* *Fiber optional:* 1Gbps & 10Gbps SM or MM
IPv6	*Real - time traffic monitoring for both* IPv4 & IPv6 *traffic, is via logs, active connections, and instantaneous bandwidt*	*Real - time traffic monitoring for both* IPv4 & IPv6 *traffic, is via logs, active connections, and instantaneous bandwidt*
# Conexiones	2.000.000	3.000.000
Costo [27]	**$11.500,00**	**$15.000,00**

Con el equipo AC504 se garantiza un crecimiento a futuro de hasta 32000 suscriptores. El equipo podrá entregar un ancho de banda en full dúplex de 200 Mbps y lo más importante es que este equipo permite trabajar con Doble Pila.

3.6.2 Equipos nuevos para la red de Distribución

Según el análisis realizado anteriormente, se detectó que todos los equipos de este segmento de red no soportan IPv6, para lo cual se planteó, como segunda

alternativa, reemplazar todos los equipos de radio existentes en la red de Distribución.

Para considerar las marcas de los fabricantes de equipos de radio que trabajen bajo el estándar 802.11 y que presten las mismas características o superiores, se debe analizar en primer lugar la distancia entre nodos (ver Tabla 3.39), y en segundo lugar características técnicas para garantizar un enlace estable y que no afecte al cliente final.

Tabla 3.39 Distancia entre los nodos de la Red de Distribución

DESDE	HACIA	EQUIPO	DISTANCIA
TWIN TOWERS	ATUCUCHO	AIRMUX 200	7,29 KM
TWIN TOWERS	GONZÁLEZ SUÁREZ	AIRMUX 200	1,46 KM
TWIN TOWERS	BUENOS AIRES	AIRMUX 400	4,14 KM
TWIN TOWERS	ATACAZO	TELETRONICS TT5800	20,38 KM
TWIN TOWERS	PUENGASÍ	AIRMUX 200	9,6 KM
ATACAZO	GUANGO	TELETRONICS TT5800	64,81 KM
GUANGO	PILISURCO	AIRMUX 400	33,72 KM
GUANGO	QUILOTOA	AIRMUX 400	26,91 KM
PUENGASÍ	AMAGUAÑA	TELETRONICS TT5800	13,76 KM
PUENGASÍ	MONJAS	AIRMUX 200	5,34 KM
PUENGASÍ	PAQUISHA	TELETRONICS TT5800	10,94 KM
BUENOS AIRES	SAN JOAQUÍN	AIRMUX 200	36,22 KM
SAN JOAQUÍN	POROTOG	TELETRONICS TT5800	15,23 KM
POROTOG	SANTA MÓNICA	AIRMUX 200	18,09 KM
SANTA MÓNICA	IMANTAG	AIRMUX 400	26,20 KM
IMANTAG	OTAVALO	AIRMUX 200	13,63 KM
OTAVALO	COTAMA	AIRMUX 200	1,26 KM
IMANTAG	IBARRA	TELETRONICS TT5800	21,32 KM
POROTOG	SILVERIO	AIRMUX 200	13,9 KM
ATUCUCHO	SAN JUAN DE CALDERÓN	AIRMUX 200	10,12 KM
SAN JUAN DE CALDERÓN	SAN JOSÉ DE MINAS	TELETRONICS TT5800	30,83 KM
SAN JUAN DE CALDERÓN	COMITÉ DEL PUEBLO	TELETRONICS TT5800	4,80 KM

En la Tabla 3.40, se presentan los equipos de radio actuales y las nuevas propuestas para reemplazar los equipos que no soportan IPv6.

Los radios de las marcas “Mikrotik” y “Ubiquiti” tienen soporte local y por lo tanto cuentan con garantía a nivel nacional.

La marca “Altai Super WiFi” es un producto que se lo debe importar desde México, por lo que el costo referencial subiría por valores de desaduanización y transporte; este equipo no tiene soporte local y cualquier desperfecto o anomalía en el equipo, requerirá enviarlo al exterior para tramitar su garantía.

Tabla 3.40 Propuestas para equipos en la Red de Distribución

IPv6	MARCA	EQUIPO	BANDA DE FRECUENCIA [GHz]	THROUGHPUT [Mbps]	ALCANCE [Km]	COSTO
Equipos sin IPv6	**AIRMUX**	200	5.3/5.4/5.8 GHz, 4.9 GHz, and 2.4 GHz	48 Mbps	80 KM	**N/A**
	AIRMUX	400	2.3 to 2.5 GHz, 3.5 licensed and 4.8 to 5.9 GHz	200 Mbps	120 km	**N/A**
	TELETRINICS	TT 5800	5.725 - 5.850GHz	54 Mbps	32 km	**N/A**
Equipos con IPv6	**MIKROTIK**	SXT5HPND	5.875GHz	550 Mbps	60 Km	**$59,00** [28]
	ALTAI SUPER WIFI	A2e	5.15-5.35, 5.47-5.725, 5.725-5.825 GHz	450 Mbps	50 km	**$59,94** [29]
	UBIQUITI	Rocket Titanium M5	5.1-5.8GHz	500 Mbps	70 km	**$129,00** [30]

Considerando lo expuesto, se debe elegir entre los 2 productos que se los encuentra a nivel nacional, y para lo cual, se considerará garantía de equipos, costo de antenas externas y administración de equipos. (Ver Tabla 3.41).

Según la Tabla 3.41, y basándose en las necesidades técnicas de los equipos, se recomienda utilizar radios de la marca Mikrotik para enlaces con distancias máximas de 30 km.

Los enlaces con distancias mayores, se recomienda utilizar los radios de la marca Ubiquiti con antena Rocket externa para aumentar la ganancia.

Tabla 3.41 Comparación equipos de Radio

	MIKROTIK SXT5HPND	UBIQUITI Rocket Titanium M5
COSTO EN ECUADOR	$59	$129
GARANTÍA	1 AÑO	1 AÑO
ANTENAS EXTERNAS	NO	SI opcional
TIPO	N/A	Rocket Dish Parabólica ($120)
GANANCIA MÁXIMA	16dbi	30 dbi
POTENCIA MÁXIMA	31 dbm (1250 mW)	27 dbm
TEMPERATURA DE TRABAJO	`-30 - 70	`-30 - 75
ÁNGULO DE COBERTURA	90 Grados	90 - 120 GRADOS
SOFTWARE DE ADMINISTRACIÓN CON IPv6	Level4 AP license	airMAX technology desde la versión 5.6.1

Según lo analizado se plantea utilizar los dos modelos de equipos dependiendo de cada tipo de enlace.

La Tabla 3.42 indica cómo sería la asignación de los equipos.

3.6.3 Equipos nuevos para la red de Acceso

Según el análisis realizado con ayuda de la Tabla 3.36, se detectó lo siguiente:

- 28 *routers* Cisco 2610 instalados el IOS 12.3(1) con soporte IPv6.
- 30 *routers* Cisco 1721 instalados el IOS 12.3(4)T4 con soporte IPv6.
- 167 *routers* Cisco 1711 instalados el IOS 12.2(15)ZL con soporte IPv6.
- 45 *routers* D-Link Dir 600 instalados el ios 1.04 con soporte IPv6.
- 2 radios *Alvarion Breeze Access* VL 5.8 sin soporte IPv6 (Equipo capa 1).

- 388 radios *Ubiquiti nano Bridge* M5 con *firmware* 5.1.2 instalados. Se requiere actualizar el *firmware* a la versión 5.6.1 para el soporte IPv6.
- 60 radios *Ubiquiti Bullet* M5 con *firmware* 5.5 instalados. Se requiere actualizar el *firmware* a la versión 5.6.1 para el soporte IPv6.
- 54 radios *Ubiquiti Nano Station* 5 sin soporte IPv6.
- 36 radios *Ubiquiti Power Station* 5 sin soporte IPv6.

Tabla 3.42 Equipos a utilizar en cada enlace según la distancia

DESDE	HACIA	EQUIPO	DISTANCIA
TWIN TOWERS	ATUCUCHO	MIKROTIK SXT5HPND	7,29 KM
TWIN TOWERS	GONZÁLEZ SUÁREZ	MIKROTIK SXT5HPND	1,46 KM
TWIN TOWERS	BUENOS AIRES	MIKROTIK SXT5HPND	4,14 KM
TWIN TOWERS	ATACAZO	MIKROTIK SXT5HPND	20,38 KM
TWIN TOWERS	PUENGASÍ	MIKROTIK SXT5HPND	9,6 KM
ATACAZO	GUANGO	UBIQUITI Rocket Titanium M5	64,81 KM
GUANGO	PILISURCO	UBIQUITI Rocket Titanium M5	33,72 KM
GUANGO	QUILOTOA	MIKROTIK SXT5HPND	26,91 KM
PUENGASÍ	AMAGUAÑA	MIKROTIK SXT5HPND	13,76 KM
PUENGASÍ	MONJAS	MIKROTIK SXT5HPND	5,34 KM
PUENGASÍ	PAQUISHA	MIKROTIK SXT5HPND	10,94 KM
BUENOS AIRES	SAN JOAQUÍN	UBIQUITI Rocket Titanium M5	36,22 KM
SAN JOAQUÍN	POROTOG	MIKROTIK SXT5HPND	15,23 KM
POROTOG	SANTA MÓNICA	MIKROTIK SXT5HPND	18,09 KM
SANTA MÓNICA	IMANTAG	MIKROTIK SXT5HPND	26,20 KM
IMANTAG	OTAVALO	MIKROTIK SXT5HPND	13,63 KM
OTAVALO	COTAMA	MIKROTIK SXT5HPND	1,26 KM
IMANTAG	IBARRA	MIKROTIK SXT5HPND	21,32 KM
POROTOG	SILVERIO	MIKROTIK SXT5HPND	13,9 KM
ATUCUCHO	SAN JUAN DE CALDERÓN	MIKROTIK SXT5HPND	10,12 KM
SAN JUAN DE CALDERÓN	SAN JOSÉ DE MINAS	UBIQUITI Rocket Titanium M5	30,83 KM
SAN JUAN DE CALDERÓN	COMITÉ DEL PUEBLO	MIKROTIK SXT5HPND	4,80 KM

Según lo indicado, se debe realizar lo siguiente:

- Cambiar 92 equipos de radio para el soporte IPv6.
- Actualizar *firmware* de 448 radios Ubiquiti a la versión 5.6.1 o superior.

Se recomienda utilizar los equipos de radio modelo Mikrotik SXT5HPND recomendados para la red de distribución.

La actualización de los radios “Ubiquiti Nano Bridge M5” y “Ubiquiti *Bullet* M5” se realiza de la siguiente manera:

1. El *firmware* se lo descarga desde la página oficial de Ubiquiti Networks [31].

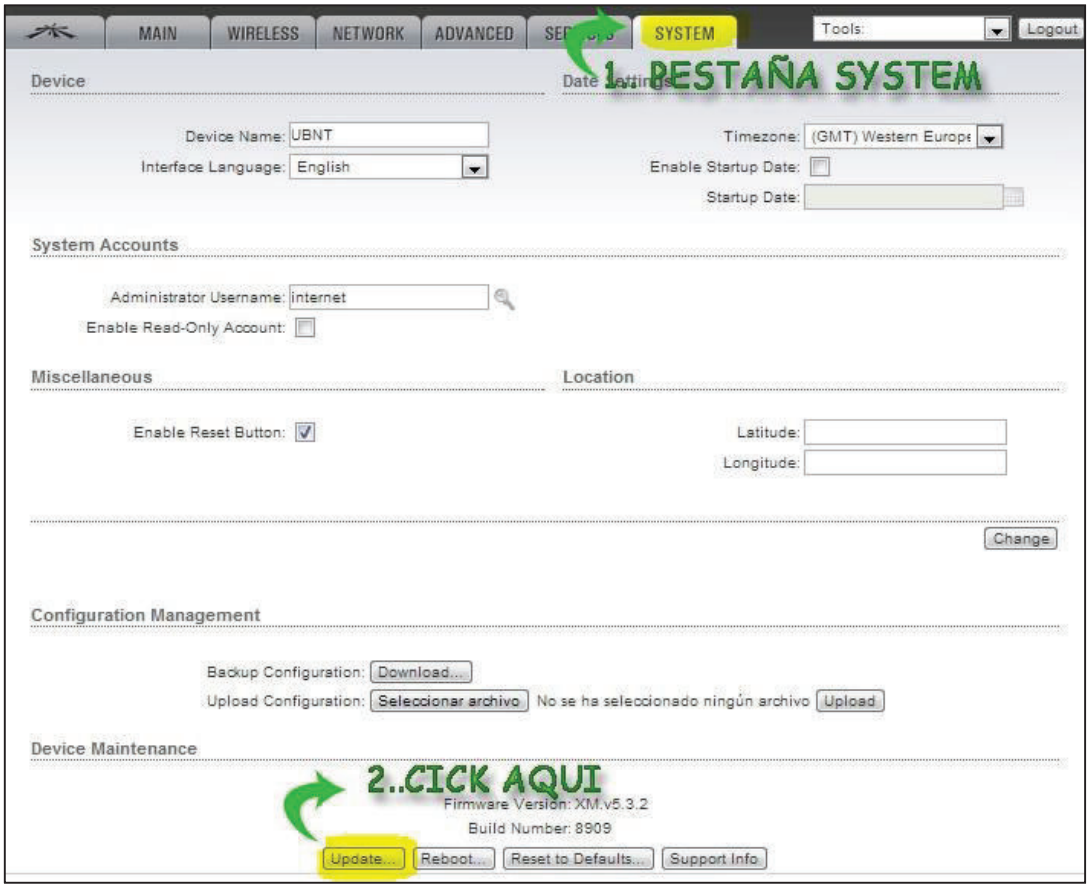


Figura 3.9 Proceso para Actualizar Firmware Ubiquiti una vez descargado archivo

2. Una vez descargado, se lo debe subir en la página de administración del equipo y seleccionar la pestaña "*System*" Ver Figura 3.9.

3. Seleccionar el archivo que se descargó, como lo muestra la Figura 3.10, hacer *click* en "*Open*" y en la siguiente ventana seleccionar "*Upload*".

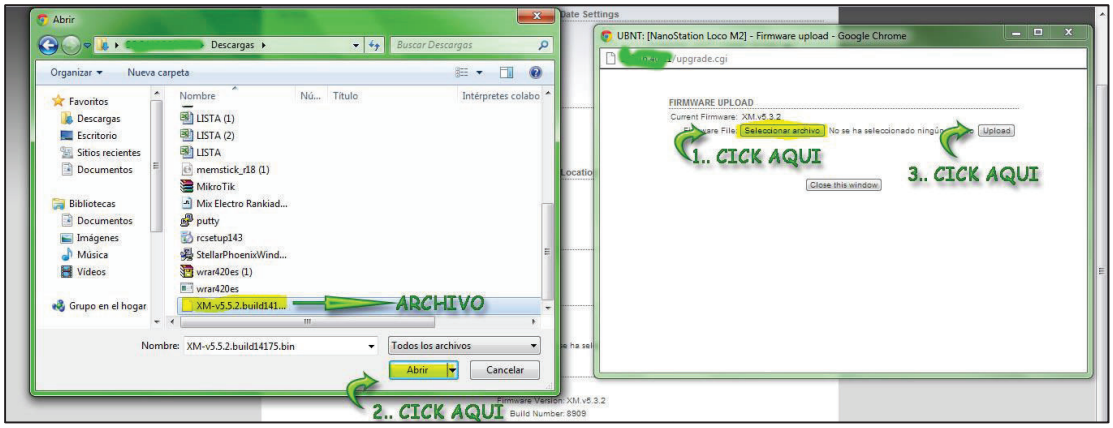


Figura 3.10 Selección del archivo para actualizar firmware Ubiquiti

4. Indicará en una nueva ventana la versión actual y la posterior, Ver Figura 3.11.

5. Esperar que el nuevo *firmware* se cargue al equipo y finalmente verificar la versión instalada.

Figura 3.11 Versión antes de Actualizar el Firmware de Ubiquiti

3.7 CONFIGURACIÓN DE EQUIPOS

La configuración de los equipos se mostrará desde el *Core* hasta el usuario final.

3.7.1 EQUIPOS DE *CORE*

Hay 6 tipos de equipos en la red de *Core* y se destallará cada uno de ellos.

Los comandos presentados son para equipos Cisco y permitirán trabajar en Doble Pila.

3.7.1.1 *Router* Cisco 2921K9

Los Cisco 2921K9 son los utilizados para conectar la red de Ecuaonline S.A. con el proveedor IPv6. En la Figura 3.12 se ve el esquema que se necesitará configurar.

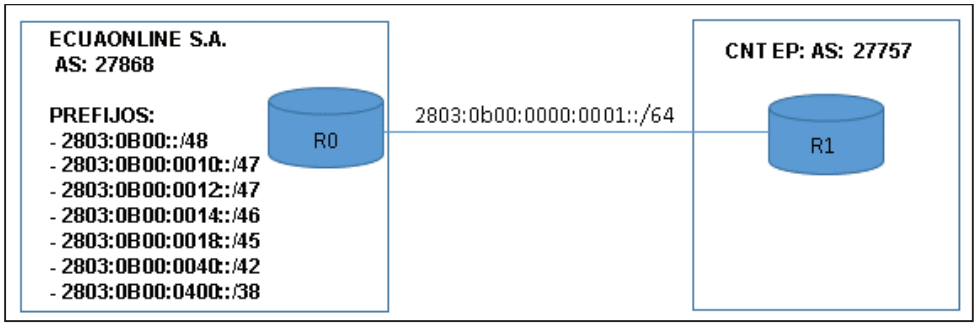


Figura 3.12 Esquema de la red a configurar

La configuración de este equipo es de la siguiente manera:

Para R0 -> Ecuaonline S.A.

```
pv6 unicast-routing
!--- Enables forwarding of IPv6 packets.
IPv6 cef
interface Loopback10
no ip address
IPv6 address 2803:0b00::/38
IPv6 enable
```

```
!
interface FastEthernet0/0
no ip address
duplex auto
speed auto
IPv6 address 2803:0b00:0:1::/64 eui-64
IPv6 enable
!
router bgp 1
bgp router-id 1.1.1.1
no bgp default ipv4-unicast
!--- Without configuring ""no bgp default ipv4-unicast"" only IPv4 will
be
!--- advertised
bgp log-neighbor-changes
neighbor 2803:0b00:0:1:C601:10FF:FE58:0 remote-as 2
!
address-family IPv6
neighbor 2803:0b00:0:1:C601:10FF:FE58:0 activate
network 2803:0b00::/48
network 2803:0b00:0010::/47
network 2803:0b00:0012::/47
network 2803:0b00:0014::/46
network 2803:0b00:0018::/45
network 2803:0b00:0040::/42
network 2803:0b00:0400::/38
network 190.123.0.0 mask 255.255.240.0
network 190.123.0.0 mask 255.255.255.0
network 190.123.1.0 mask 255.255.255.0
network 190.123.2.0 mask 255.255.255.0
network 190.123.3.0 mask 255.255.255.0
network 190.123.4.0 mask 255.255.255.0
network 190.123.5.0 mask 255.255.255.0
network 190.123.6.0 mask 255.255.255.0
network 190.123.7.0 mask 255.255.255.0
network 190.123.8.0 mask 255.255.255.0
network 190.123.9.0 mask 255.255.255.0
network 190.123.10.0 mask 255.255.255.0
network 190.123.11.0 mask 255.255.255.0
network 190.123.12.0 mask 255.255.255.0
```

```
network 190.123.13.0 mask 255.255.255.0
network 190.123.14.0 mask 255.255.255.0
network 190.123.15.0 mask 255.255.255.0
network 200.110.232.0 mask 255.255.248.0
network 200.110.232.0 mask 255.255.255.0
network 200.110.233.0 mask 255.255.255.0
network 200.110.234.0 mask 255.255.255.0
network 200.110.235.0 mask 255.255.255.0
network 200.110.236.0 mask 255.255.255.0
network 200.110.237.0 mask 255.255.255.0
network 200.110.238.0 mask 255.255.255.0
network 200.110.239.0 mask 255.255.255.0
neighbor 2800:0370::64 remote-as 27757
neighbor 2800:0370::64 description CNT
no auto-sumary
interface GigabitEthernet0/0
description trunk-cnt
IPv6 address 2800:0370::64
exit-address-family
```

3.7.1.2 *Switch* Catalyst WS-C3750G-24T

Los Cisco Catalyst WS3750G-24T son los utilizados para conectar la red de Ecuaonline S.A. con los proveedores de Internet. Este equipo también se utiliza para conectar las redes Intranet, Metro *Ethernet*.

```
Switch(config)# sdm prefer dual-ipv4-and-IPv6 default
Switch(config)# ip routing
Switch(config)# IPv6 unicast-routing
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# no switchport
Switch(config-if)# ip address 200.110.232.0 255.255.248.0
Switch(config-if)# ip address 190.123.0.0 255.255.255.0
Switch(config-if)# IPv6 address 2803:0b00:0:1::/64 eui 64
Switch(config-if)# end
Switch# configure terminal
Switch(config)# IPv6 dhcp pool cayambe
Switch(config-dhcpv6)#address prefix 2803:0b00:0014::/46
Switch(config-dhcpv6)# end
```

```
Switch(config)# IPv6 dhcp pool ibarra
Switch(config-dhcpv6)#address prefix 2803:0b00:0010::/47
Switch(config-dhcpv6)# end
Switch(config)# IPv6 dhcp pool otavalo
Switch(config-dhcpv6)#address prefix 2803:0b00:0012::/47
Switch(config-dhcpv6)# end
Switch(config)# IPv6 dhcp pool latacunga
Switch(config-dhcpv6)#address prefix 2803:0b00:0018::/45
Switch(config-dhcpv6)# end
Switch(config)# IPv6 dhcp pool business-datos
Switch(config-dhcpv6)#address prefix 2803:0b00:0040::/42
Switch(config-dhcpv6)# end
Switch(config)# IPv6 dhcp pool quito
Switch(config-dhcpv6)#address prefix 2803:0b00:0400::/38
Switch(config-dhcpv6)# end
Switch(config)# IPv6 dhcp pool intranet
Switch(config-dhcpv6)#address prefix 2803:0b00::/48
Switch(config-dhcpv6)# end
```

3.7.2 EQUIPOS DE DISTRIBUCIÓN

La configuración IPv6 en los equipos de radio que se sugiere adquirir se analiza a continuación.

3.7.2.1 Mikrotik SHT5HPND

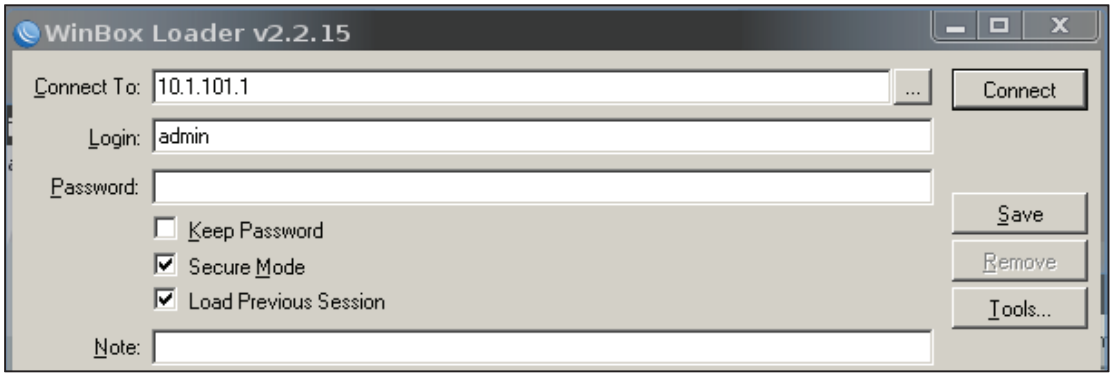


Figura 3.13 Inicio del programa WinBox

Para la administración de este equipo es necesario descargar el programa de administración llamado *WinBox* desde la *web* del autor [32], comprobar que la descarga sea de la versión V5RC6 que soporta IPv6. Una vez descargado se inicia el programa y se pedirá que ingrese la dirección IP del dispositivo que se haya conectado. (Ver Figura 3.13).

Cuando se ingresan las credenciales de acceso, se desplegará la ventana de herramientas del programa, según se puede ver en la Figura 3.14.

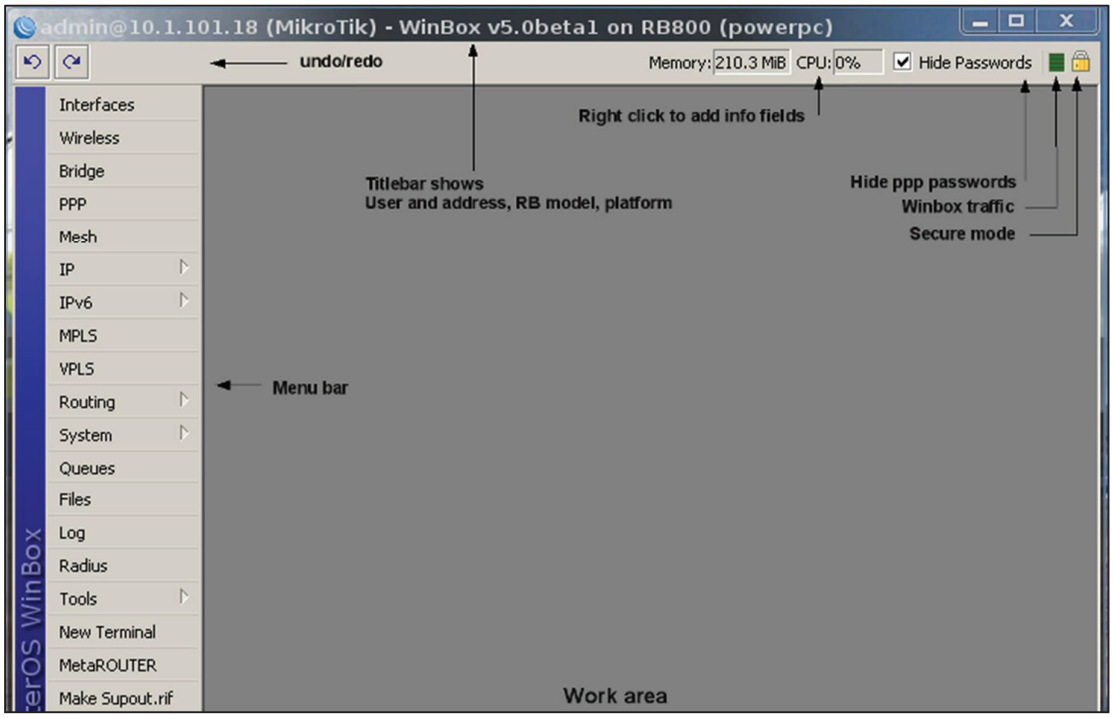


Figura 3.14 Ventana de herramientas del programa WinBox V5RC6

En esta ventana se puede configurar IPv6 presente en la barra de menú.

3.7.2.2 Ubiquiti Rocket Titanium M5

Para la configuración de IPv6 en los radios Ubiquiti Rocket Titanium M5 o similares, se debe utilizar como mínimo la versión de *firmware* 5.6.1. La interfaz de un equipo Ubiquiti con este *firmware* se presenta con la Figura 3.15.

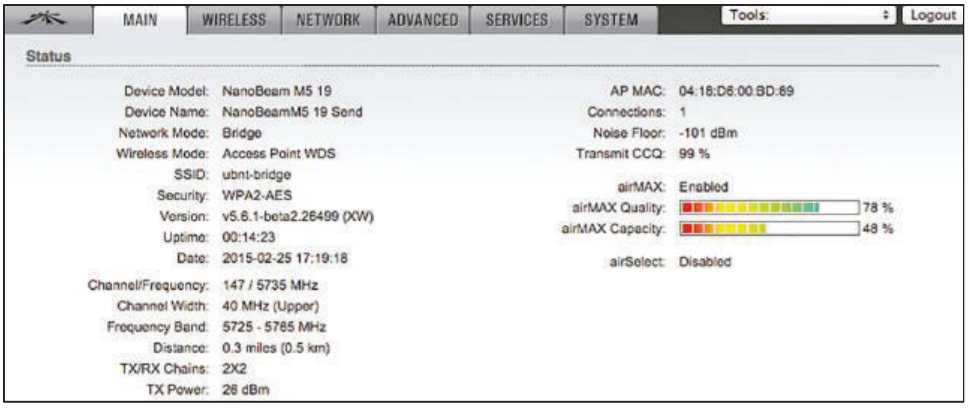


Figura 3.15 Pantalla de inicio de *AirOS*

Para direccionamiento IPv6, la configuración de la interfaz del *AirOS* soporta Doble Pila y el formato IPv6 está aceptado por el *firmware*. La configuración IPv6 se habilita directamente en la interfaz gráfica del IOS. Aquí se puede elegir entre SLAAC (*StateLess Address Auto-Configuration*) o manual. (Ver Figura 3.16).

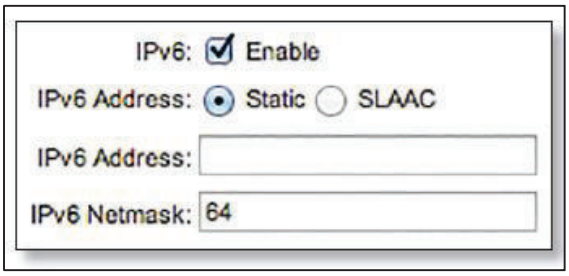


Figura 3.16 Configuración IPv6 en *AirOS*

Para la configuración *WAN* se debe seleccionar IPv6 y escoger en IPv6 estática o IPv6 SLAAC, tal como se muestra en la Figura 3.17.

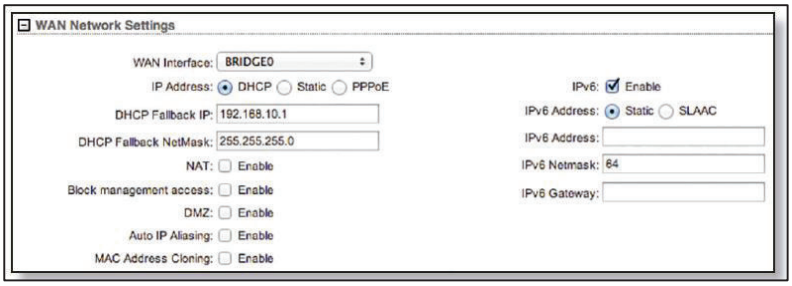


Figura 3.17 Configuración IPv6 para *WAN*

3.7.3 EQUIPOS DE ACCESO

En este segmento de red se verá la configuración del *Router* Dlink Dir600 para configurarlo en IPv6.

Las configuraciones de los equipos Cisco y radios Ubiquiti y Mikrotik ya se explicaron anteriormente.

3.7.3.1 Equipo Dlink Dir 600

El CPE de usuario Dlink Dir 600 tiene cargado en su versión 2.10 la funcionalidad del protocolo IPv6. Para poder habilitar esta característica se debe seleccionar la opción IPv6 en la barra de menús, y escoger el tipo de conexión WAN que tenga el cliente. Puede ser por DHCPv6 o SLAAC. Ver Figura 3.18.

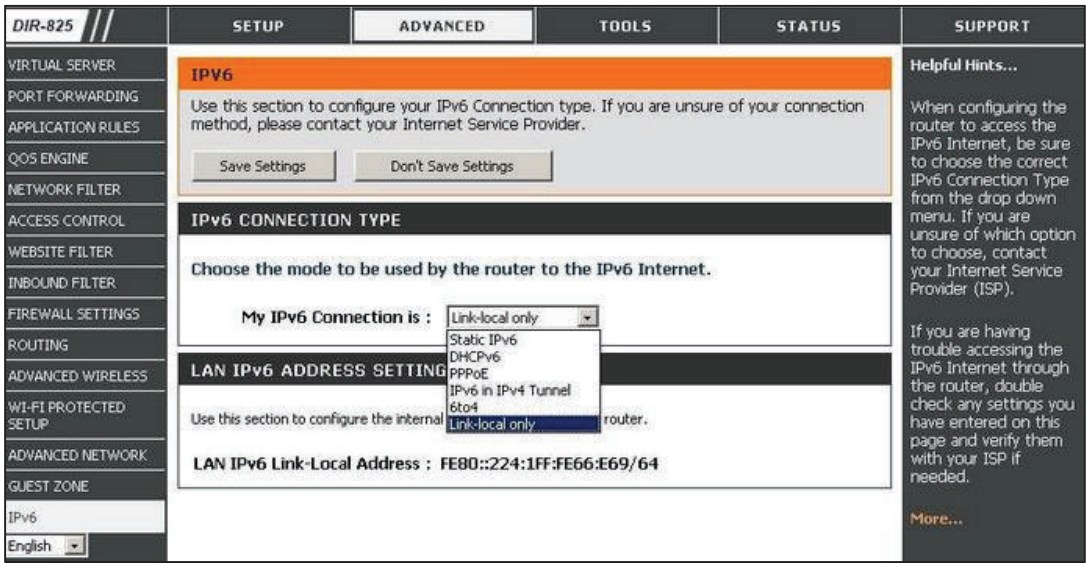


Figura 3.18 Configuración IPv6 en Dlink Dir 600

Con estas configuraciones, todos los equipos soportarán IPv6 e IPv4 simultáneamente, por lo que se podrá trabajar en Doble Pila.

Con la configuración de los equipos descritos en cada segmento de red, se garantiza el correcto funcionamiento de la red con el protocolo IPv6 en Doble Pila.

CAPÍTULO 4

ESTUDIO DE COSTOS

Según el análisis realizado en los capítulos anteriores, se detallará el costo total que tendría implementar el proyecto actual.

Para poder determinar el costo total se dividirá en costos unitarios o por segmentos de la red.

4.1 COSTO DEL PROYECTO

Para determinar el ancho de banda requerido al proveedor, y con eso solicitar la cotización, se requiere conocer previamente el ancho de banda contratado para los usuarios en IPv4. En la Tabla 4.1 se observa el ancho de banda que tiene contratado cada usuario para el servicio de Internet y datos en IPv4.

Tabla 4.1 Ancho de banda por usuario

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
NODO TWIN TOWERS				
CREA COMUNICACIONES	Internet	1,500		
MIGRACIÓN RELACIONES EXTERIORES	Internet	0,500		
COMERCIO ITALIANA	Internet	0,500		
PROLIFE	Internet	0,125		
PENCAFLOR	Internet	0,250		
COMDIGITRONIX	Internet	0,750		
SNOB UIO (1/4)	Internet	1,250	Datos	0,5
VH COMUNICACIONES	Internet	0,500		
BIOALIMENTAR QUITO (1/2)	Internet	1,500	Datos	0,25
ESTUDIO JURÍDICO NOBOA PEÑA Y LARREA	Internet	0,250		
RAÚL REVELO (GALLERY ABOGADOS)	Internet	0,500		
ECUANROSES ARCOIRIS (1/4)	Internet	1,500	Datos	0,5

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
RADISIS	Internet	0,250		
DIRECCION NACIONAL DE MIGRACIÓN	Internet	0,250		
FIDU ECUADOR	Internet	0,500		
ABP PUBLICIDAD	Internet	0,250		
AMAZON	Internet	2,000		
WORLD ECUADOR (WORLD MATRIZ)	Internet	0,500		
NODO BUENOS AIRES				
FLORES CELESTIALES	Internet	0,250		
SANTILLÁN BORJA FRANCISCO RAFAEL	Internet	0,500		
SEVILLA AMAYA VÍCTOR HUGO (LA HUERTA)	Internet	0,500		
ARBUSTA FLORQUIN S.A. (1/4)	Internet	1,500	Datos	0,5
ECUAMERICA BRAZIL (1/2)	Internet	1,250	Datos	0,125
COMUMAP	Internet	0,500		
PAÚL AYALA	Internet	0,500		
COLEGIO AMÉRICA	Internet	0,125		
PONY CENTRAL	Internet	0,750		
INGE CABLE	Internet	0,125		
LOGIANDINA S.A.	Internet	0,500		
ELECTROBRAVER CIAL LTDA	Internet	0,500		
ESCUELA JORGE ICAZA	Internet	0,125		
INROSES 2 (1/3)	Internet	1,750	Datos	0,25
IMPRENTA MARISCAL	Internet	0,500		
REMIGIO POZO - AGRIROSE	Internet	0,750		
ARBUSTA (2/4)	Internet	1,500	Datos	0,5
NATIVE BLOOMS MONTESERRÍN	Internet	0,500		
BROWNBREDING INGENIERÍA S.A.	Internet	0,500		
MARÍA VALENTE (CAFENET MV)	Internet	0,500		
NODO GONZÁLEZ SUÁREZ				
PRODUNORTE GERENCIA (1/3)	Internet	1,750	Datos	0,25
GERENTE GALAPAGOS FLOWERS	Internet	0,500		

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
SNOB PUEMBO (2/4)	Internet	1,250	Datos	0,5
LA ROSALEDA	Internet	0,250		
FRAGMENTO HUMANO	Internet	0,500		
FLORECC	Internet	0,125		
WILMA ESCALANTE	Internet	0,125		
ROSE ELITE RIESLINGFLOWER	Internet	0,500		
VIAMERICA	Internet	0,500		
PEÑA & NOBOA PANAVIAL PIFO	Internet	0,250		
DEL CAMPO (LA HOLANDESA)	Internet	0,500		
ALIANZA FRANCESA	Internet	0,500		
VETFARM PIFO	Internet	0,250		
JUAN CARLOS PINEIDA	Internet	0,125		
ARBUSTA CUMBAYÁ (3/4)	Internet	1,500	Datos	0,5
COTA MATRIZ (1/2)	Internet	1,750	Datos	0,25
MONSERRAT MEJÍA	Internet	0,125		
CASA HUMBOLDT	Internet	0,500		
EXPOFLORES	Internet	0,125		
PILONES LA VICTORIA	Internet	0,250		
ECUAMERICA (2/2)	Internet	1,250	Datos	0,125
BRIGHTCELL MATRIZ	Internet	12,000		
BACOLOGY ULLOA (1/3)	Internet	1,000	Datos	1
MATERIA GRIS	Internet	0,500		
VENTURA MALL	Internet	0,500		
NODO ATUCUCHO				
FERNANDO SAENZ OFICINA (1/2)	Internet	1,125	Datos	0,125
FERNANDO SAENZ CASA (2/2)	Internet	1,125	Datos	0,125
FLORES EXPRESS	Internet	0,500		
BM PUBLICIDAD	Internet	0,500		
BELÉN CASARES	Internet	0,125		
RAFAEL POVEDA (COBERPACK)	Internet	0,250		
SNOB (3/4)	Internet	1,250	Datos	0,5
COTA BODEGA (2/2)	Internet	1,750	Datos	0,25
FERROMEDICA	Internet	0,250		
VEGAFLOR QUITO (1/3)	Internet	1,250	Datos	0,125

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
BANCOLOGY MATRIZ (2/3)	Internet	1,000	Datos	1
PYGANFLOR (COMITÉ DEL PUEBLO)	Internet	0,500		
VÍCTOR NAVARRO	Internet	0,125		
SJ YERSEY CENTRAL (1/3)	Internet	1,250	Datos	0,25
PATPRIMO MATRIZ (1/5)	Internet	2,500	Datos	0,5
SERVIA	Internet	0,125		
NODO SAN JUAN DE CALDERÓN				
GALAFLOR QUINCHE (1/2)	Internet	1,000	Datos	0,125
GERENTE SNOB	Internet	0,125		
COOPERATIVA DE AHORRO Y CRÉDITO SANTA ANA DE NAYÓN MATRIZ (1/3)	Internet	1,250	Datos	0,25
COOPERATIVA DE AHORRO Y CRÉDITO SANTA ANA DE NAYÓN GUALO (2/3)	Internet	1,250	Datos	0,25
COOPERATIVA DE AHOORO Y CRÉDITO SANTA ANA DE NAYÓN COMITÉ DEL PUEBLO (3/3)	Internet	1,250	Datos	0,25
PLASTIKYTO	Internet	0,500		
SJ YERSEY CALDERÓN (2/3)	Internet	1,250	Datos	0,25
NEUMAN FLOWERS	Internet	0,500		
ECUAFIORI EXPORT S.A	Internet	0,250		
SANDE	Internet	0,500		
PATPRIMO 2 (2/5)	Internet	2,500	Datos	0,5
VIOLETA FLOWERS	Internet	0,500		
HILSEA CHIVAN	Internet	0,250		
MARCO CUEVA	Internet	0,250		
JOSÉ LUIS GUAMÁN	Internet	0,250		
ALIMENTOS SUPERIOR PLANTA	Internet	0,250		
ELENA YAKLOVEVA	Internet	0,250		
FLORES DE LA COLONIA (FLODECOL2) (1/3)	Internet	2,000	Datos	0,5
HACIENDA VERDE	Internet	0,125		
PIANGO FLOR S.A.	Internet	0,250		
CAPSYD MALCHINGUI	Internet	0,250		
CARLOS MANTILLA	Internet	0,250		
HISLEA PERUCHO	Internet	0,125		

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
COACSA LUMBISI	Internet	0,500		
COLEGIO MALCHINGUI	Internet	0,500		
JUNTA PARROQUIAL MALCHINGUI	Internet	0,500		
NODO COMITÉ DEL PUEBLO				
IMBAUTO DISMARK (1/5)	Internet	1,500	Datos	1
ROOSVELT MONCAYO	Internet	0,500		
NODO PUENGASÍ				
IVAN RUIZ	Internet	0,250		
INFLOWERS	Internet	0,250		
JAVI CORONEL	Internet	0,250		
INMOVILIARIA VERZAM (CARLOS VERA)	Internet	0,500		
VVK ALIMENTOS	Internet	0,125		
COLEGIO MONTEBELLO	Internet	0,125		
BASURTO CORNEJO NOELIA GENOVEVA	Internet	0,500		
KEVIN VALLE	Internet			
JUAN DIEGO ALMACHE	Internet	0,500		
PATPRIMO ECUADOR COMERCIALIZADORA S.A. (3/5)	Internet	2,500	Datos	0,5
HOSTERIA RANCHO DEL CIELO	Internet	0,500		
ELIMED	Internet	0,125		
UNION VERA PLASTIK	Internet	0,250		
CARLOS LLUMIQUINGA	Internet	0,250		
NODO MONJAS				
FLOREQUISA (1/3)	Internet	2,500	Datos	0,5
NODO PAQUISHA				
ECOROSES	Internet	0,250		
SNOB (4/4)	Internet	1,250	Datos	0,5
NODO AMAGUAÑA				
TEXTIL ECUADOR	Internet	0,125		
LATACUNGA				
NODO QUILOTOA				
ROSE SUCCESS	Internet	0,250		
CARLOS MARTINEZ	Internet	0,250		
HOTEL JULIO SAN PEDRO	Internet	0,500		

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
CHANGOLUISA IZA ROSA MARÍA	Internet	0,125		
MARÍA PILA	Internet	0,250		
EASTMANROSES CASA	Internet	0,125		
LUIS CHANCUSI	Internet	0,250		
HISPANO ROSE	Internet	0,125		
UNIDAD EDUCATIVA FAE 5	Internet	0,500		
CURTILAN	Internet	0,250		
FUNDACION SIERRA FLOR	Internet	0,750		
ROSAS DEL COTOPAXI	Internet	0,250		
FLORICOLA EASTMAN ROSES	Internet	0,125		
ESCUELA DE PERFECCIONAMIENTO DE AEROTÉCNICOS	Internet	0,250		
MARLEN ROSES (1/2)	Internet	1,250	Datos	0,125
ROSELY FLOWERS	Internet	0,250		
LA CIENEGA	Internet	0,500		
RAMIRO MENA	Internet	0,125		
TOP ROSES	Internet	0,250		
SIERRA FLOR (1/2)	Internet	1,500	Datos	0,25
AGRONPAXI	Internet	0,500		
CASA JULIO SAN PEDRO	Internet	0,250		
RADIO OASIS	Internet	0,500		
JUAN CARLOS TOAPANTA	Internet	0,125		
COMPUWORLD 1	Internet	0,500		
KARINA GUANOLUISA	Internet	0,250		
NODO GUANGO				
ISINCHE FLOWERS	Internet	0,250		
NELLY VACA	Internet	0,125		
RAÚL LEON	Internet	0,500		
WASINGTON ACURIO	Internet	0,250		
AZERI FLOWERS	Internet	0,500		
MERIZALDE	Internet	0,125		
COLEGIO POALO	Internet	0,250		
GLORIA MARÍA PUCO	Internet	0,250		
MARLEN ROSES 2 (2/2)	Internet	1,250	Datos	0,125
SANBEL FLOWERS	Internet	0,250		
ACOLIT ASESORES Y CONSULTORES DEL LITORAL	Internet	0,500		
FERNANDO EASTMAN	Internet	0,125		

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
FLORES DE TOACAZO	Internet	0,250		
HACIENDA TAMBO	Internet	0,750		
PRESIDENCIA SIERRA FLOR	Internet	0,500		
INORFLOWERS	Internet	0,500		
PILVICSA	Internet	0,125		
LA ROSALEDA	Internet	0,500		
ECUANROSES ARCOFLOR (2/4)	Internet	1,500	Datos	0,5
ECUANROSES MATRIZ (3/4)	Internet	1,500	Datos	0,5
ECUANROSES GROWERFARM (4/4)	Internet	1,500	Datos	0,5
SIERRA FLOR MATRIZ (2/2)	Internet	1,500	Datos	0,25
SPACIUM	Internet	0,250		
LOCOAM FARMS	Internet	0,500		
ESCUELA OSWALDO BONILLA	Internet	0,250		
TAMBO 2 (2/2)	Internet	1,000	Datos	0,125
TAMBO 1 (1/2)	Internet	1,000	Datos	0,125
NODO PILISURCO				
BIOALIMENTAR (2/2)	Internet	1,500	Datos	0,25
INCUBANDINA	Internet	0,500		
PAT PRIMO AMBATO (4/5)	Internet	2,500	Datos	0,5
BANCOLOGY (3/3)	Internet	1,000	Datos	1
YUYAK RUNA	Internet	0,250		
IBARRA				
NODO IMANTAG				
SACHS STEINHARDT BETTY JILL	Internet	0,250		
MUSHUK PAKARY COTACACHI (1/3)	Internet	1,750	Datos	0,25
PAT PRIMO ATUNTAQUI (5/5)	Internet	2,500	Datos	0,5
DJNET	Internet	0,500		
LA UNICA 2 (2/3)	Internet	2,000	Datos	0,5
INROSES COTACACHI (2/3)	Internet	1,750	Datos	0,25
SOFIA BENAVIDES	Internet	0,250		
LA UNICA 1 (1/3)	Internet	2,000	Datos	0,5
PENCAFLOR	Internet	0,500		
LA UNICA 3 (3/3)	Internet	2,000	Datos	0,5
SJ JERSEY (3/3)	Internet	1,250	Datos	0,25
RED ESCOLAR COTACACHI	Internet	0,250		

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
MUSHUK PAKARI MATRIZ (2/3)	Internet	1,750	Datos	0,25
PLAZA NET	Internet	0,500		
SOLNET	Internet	0,125		
PATRICIO RUIZ	Internet	0,250		
JORGE DAVILA	Internet	0,250		
NODO IBARRA				
SANTIAGO COLLAGUAZO (PUERTA VIRTUAL)	Internet	0,500		
FLORES DEL AMAZONAS	Internet	0,250		
IMBAUTO GALPON (2/5)	Internet	1,500	Datos	1
IMBAUTO SOLO CHEVROLET (3/5)	Internet	1,500	Datos	1
IMBAUTO IBARRA (4/5)	Internet	1,500	Datos	1
MUSHUK IBARRA (3/3)	Internet	1,750	Datos	0,25
COMERCIAL HIDROBO MATRIZ (1/5)	Internet	2,000	Datos	0,5
COMERCIAL HIDROBO AUTHESA (2/5)	Internet	2,000	Datos	0,5
COMERCIAL HIDROBO MAZDA (3/5)	Internet	2,000	Datos	0,5
COMERCIAL HIDROBO PROINTEC (4/5)	Internet	2,000	Datos	0,5
ADRIAN MERLO	Internet	0,250		
PAVEL ESCALANTE	Internet	0,250		
RADIO IMPERIO FM (1/2)	Internet	2,000	Datos	1
RADIO IMPERIO AM (2/2)	Internet	2,000	Datos	1
CASA LUIS VITERI RADIO IMPERIO	Internet	0,250		
HECTOR PILATAXI	Internet	0,250		
HOTEL LA GIRALDA	Internet	0,500		
KATIA POZO	Internet	0,125		
OTAVALO				
NODO COTAMA				
COLEGIO TÉCNICO REPUBLICA DEL ECUADOR	Internet	0,500		
PATRICIO SAAVEDRA	Internet	0,250		
NELLY PINEDA 2 (2/2)	Internet	2,000	Datos	0,5
NELLY PINEDA (1/2)	Internet	2,000	Datos	0,5
IMBAUTO OTAVALO (5/5)	Internet	1,500	Datos	1

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
HOSTAL MAY SHIS	Internet	0,250		
INSTITUTO TÉCNICO OTAVALO	Internet	0,500		
ALEXIS MORA	Internet	0,125		
RED EDUCATIVA QUICHINCHE	Internet	0,500		
CAYAMBE				
NODO SAN JOAQUÍN				
NELLYS FLOWERS	Internet	0,500		
FLOREQUISA (2/3)	Internet	2,500	Datos	0,5
FLOREQUISA VENTAS (3/3)	Internet	2,500	Datos	0,5
ARBUSTA (4/4)	Internet	1,500	Datos	0,5
SAN BENITO	Internet	0,500		
EXXIDE	Internet	0,250		
INROSES (3/3)	Internet	1,750	Datos	0,25
LUXUSBLUMEN	Internet	0,500		
PICASO FLOWERS	Internet	0,250		
HENRY SIERRA	Internet	0,125		
ECUAMADRIGAL	Internet	0,500		
ANNIROSES	Internet	0,500		
GALAFLOR (2/2)	Internet	1,000	Datos	0,125
CYBORNET	Internet	0,125		
NODO SILVERIO				
FLODECOL (2/3)	Internet	2,000	Datos	0,5
FLORES DE LA COLINA (3/3)	Internet	2,000	Datos	0,5
MANUEL BUITRON	Internet	0,250		
TURIS AGRONELPO	Internet	0,250		
NODO POROTOG				
COMERCIAL HIDROBO (5/5)	Internet	2,000	Datos	0,5
MARUSROSES	Internet	0,250		
DIRECCION PROVINCIAL BILINGUE	Internet	0,500		
DIRECCION PROVINCIAL AMBIENTE	Internet	0,500		
EMAP PEDRO MONCAYO	Internet	0,125		
BRIHANNA	Internet	0,250		
JUAN CARLOS OBANDO	Internet	0,250		
JUNTA PARROQUIAL LA ESPERANZA	Internet	0,500		
MYSTIC FLOWERS	Internet	0,125		

NOMBRES	SERVICIO 1 COMPARTICIÓN 8:1	AB SERVICIO 1 [MBPS]	SERVICIO 2 COMPARTICIÓN 2:1	AB SERVICIO 2 [MBPS]
FIORENTINA	Internet	0,250		
ANNIROSES CASA	Internet	0,250		
ROSADEX	Internet	0,500		
JUNTA PARROQUIAL TOCACHI	Internet	0,125		
FLOWERFEST	Internet	0,250		
NELGOR	Internet	0,125		
PRODUNORTE AGRONATURA (2/3)	Internet	1,750	Datos	0,25
AGRITAB 2	Internet	0,500		
NODO SANTA MÓNICA				
HACIENDA GUACHALA	Internet	0,250		
SANTA ANA	Internet	0,500		
NUCLEO DE FLORICULTORES	Internet	0,500		
MAURICIO TARANTO CEVALLOS	Internet	0,250		
RIOROSES	Internet	0,500		
PRODUNORTE AYORA (3/3)	Internet	1,750	Datos	0,25
VEGA FLOR TUPIGACHI (2/3)	Internet	1,250	Datos	0,125
VEGA FLOR SAN PABLO (3/3)	Internet	1,250	Datos	0,125
TOTAL	**Internet**	**212,500**	**Datos**	**33,375**

Ecuaonline S.A. tiene paquetes de Internet desde 0,125 Mbps hasta el más grande que entrega a Brighcell de 20 Mbps. El servicio de Internet tiene compartición de 8:1 en su gran mayoría, pero también ofrece paquetes dedicados para los clientes que requieran el servicio. El total de ancho de banda (AB) requerido para todos los usuarios de Internet es de 212,5 Mbps. La totalidad de ancho de banda sería necesaria contratar siempre y cuando a cada usuario se le entregue el canal dedicado. Para este caso, los usuarios usan compartición 8:1 a excepción de Brighcell que tiene 12 Mbps dedicado. El total de ancho de banda para Internet en IPv4 es de 37,06 Mbps y esta cantidad de ancho de banda se requeriría si todos los usuarios utilizaran el ancho de banda asignado al mismo tiempo. En realidad, el uso de Internet es más bajo que 37,06 Mbps para el servicio de Internet.

Ecuaonline S.A. tiene paquetes de datos desde 0,125 Mbps hasta el más grande que es de 1 Mbps. El servicio de Datos tiene compartición de 2:1 en su gran

mayoría, pero también ofrece paquetes dedicados para los clientes que requieran el servicio. El total de ancho de banda requerido para todos los usuarios de Datos es de 33,375 Mbps. La totalidad de ancho de banda sería necesaria contratar siempre y cuando a cada usuario se le entregue el canal dedicado. Para este caso, los usuarios usan compartición 2:1.

El total de ancho de banda para Datos en IPv4 es de 16,7 Mbps y esta cantidad de ancho de banda se requeriría si todos los usuarios utilizaran el ancho de banda asignado al mismo tiempo. En realidad, el uso de Datos es más bajo que 16 Mbps para el servicio de Datos.

Esto quiere decir que el ancho de banda requerido para todos los usuarios de Internet y datos con IPv4 es de 37,06 + 16,7 = 53,76 Mbps. Actualmente se tiene contratado un ancho de banda de 55 Mbps.

Considerando a la cantidad de ancho de banda utilizado en IPv4, y con la hipótesis de que al desplegar IPv6 se utilizará el servicio paulatinamente hasta llegar al cliente, se plantea adquirir un ancho de banda de máximo 20 Mbps para realizar pruebas y conexiones entre equipos. La demanda del servicio en IPv6 llevará algún tiempo y no es necesario adquirir un paquete de ancho de banda tan grande. Conforme aumente la demanda, se aumentará el ancho de banda hacia el proveedor.

Para poder mejorar el servicio hacia los clientes, se sugiere disminuir la compartición que el proveedor brinda hacia los clientes, es decir, se plantea entregar a los usuarios *business* una compartición de Internet de por lo menos 4:1, con lo cual, se entregará un mejor servicio al cliente final, la empresa estará en un nivel competitivo y se podrá promocionar el servicio de Internet con IPv6 con velocidades más elevadas para los clientes.

Considerando los factores mostrados en la Tabla 4.2 se ve que la mejor opción respecto a disponibilidad del servicio y costo mensual por el servicio de Internet IPv6 es CNT EP. Las cotizaciones realizadas se las puede consultar en la Figura C-1, C2 y C3 respectivamente, dentro del Anexo C.

Tabla 4.2 Comparación del servicio IPv6 que oferta cada ISP

	COSTO INTALACION	COSTO MENSUAL	DISPONIBILIDAD	SOPORTE TÉCNICO	MEDIO DE ACCESO
CNT EP	$300,00	$980,00	99,6 %	24 HORAS	FIBRA
TELCONET	$250,00	$2100,00	99,5 %	24 HORAS	FIBRA
CONECEL	$300,00	$1300,00	99,54 %	24 HORAS	FIBRA

Para poder obtener los costos totales resultantes del diseño en la red de *Core*, se indicarán los costos de cada componente en esta sección de red. (Ver Tabla 4.3).

Tabla 4.3 Costo de equipos y servicio de Internet para la Red de *Core*

RED DE *CORE*			
PROVEEDOR IPv6 (INSTALACIÓN INICIAL)	20 Mbps	CNT EP TELCONET CLARO	$ 300,00 $ 250,00 $ 300,00
LIMITADOR DE ANCHO DE BANDA Y GESTIÓN DE RED	NetEnforcer	AC-500	$ 5.920,00
		AC-1400	$ 20.600,00
		AC-3000	$ 47.080,00
		AC-6000	$ 49.720,00
	NetEcuaolizer	NE3000	$ 11.500,00
		NE4000	$ 15.000,00

Entre los limitadores de ancho de banda se elige al equipo NetEnforcer AC-504 por su variedad de funcionalidades descritas anteriormente y también por el costo más bajo en comparación que los otros modelos y otras marcas.

El costo de los equipos necesarios para trabajar en Doble Pila en la red de distribución está contemplados en la Tabla 4.4.

Tabla 4.4 Costo de equipos para la Red de Distribución

RED DE DISTRIBUCIÓN		
RADIOS Y ANTENAS PARA ENLACE ENTRE NODOS	MIKROTIK SXT5HPND	$ 59,00
	UBIQUITI Rocket Titanium M5	$ 129,00
	ANTENA PARABÓLICA PARA UBIQUITI Rocket Titanium M5	$ 120,00
	ALTAI SUPER WIFI	$ 59,94

Según el análisis hecho en el capítulo 3, se decide utilizar los equipos de radio Mikrotik SXT5HPND para los enlaces no mayores a 30 km y utilizar los equipos Ubiquiti Rocket Titanium M5 con su antena para enlaces mayores a 30 km.

Del mismo modo, para la red de Acceso, se utilizará el Equipo Mikrotik SXT5HPND.

Con todos estos datos se puede analizar el costo total en equipamiento para la implementación, Ver Tabla 4.5.

Tabla 4.5 Costo de equipos

#	QTY	DESCRIPCIÓN	MARCA/PROVEEDOR	PRECIO UNITARIO	PRECIO TOTAL
2	2	LIMITADOR DE ANCHO DE BANDA Y GESTIÓN DE RED	NetEnforcer AC504	$ 5.920,00	$ 11.840,00
3	18	EQUIPO DE RADIO PARA ENLACE ENTRE NODOS MENOR A 30 KM	MIKROTIK SXT5HPND	$ 59,00	$ 1.062,00
4	4	EQUIPO DE RADIO PARA ENLACE ENTRE NODOS MAYOR A 30 KM	UBIQUITI Rocket Titanium M5	$ 129,00	$ 516,00
5	4	ANTENAS PARA EQUIPO DE RADIO DE ENLACE ENTRE NODOS MAYOR A 30 KM	Rocket Dish Parabólica 5 GHz, 30 dBi Dual Pol	$ 120,00	$ 480,00
6	92	EQUIPO DE RADIO PARA ENLACE ENTRE NODOS MENOR A 30 KM	MIKROTIK SXT5HPND	$ 59,00	$ 5.428,00
COSTO TOTAL DE EQUIPOS					**$ 19.326,00**

Con el resultado económico de la Tabla 4.5, se puede conocer que se requiere invertir $19.326,00 para adquirir equipamiento que soporte *Dual Stack* para las redes de *Core* y Distribución y Acceso.

El costo de instalación del servicio IPv6 que Ecuaonline S.A deberá cancelar al Proveedor es de $300,00 y se lo realizará una sola vez al inicio del proyecto

El costo de mantenimiento mensual es de $2.743,60 e incluye el valor mensual a pagar, ver la Tabla 4.6.

Tabla 4.6 Costo mantenimiento

	COSTO MENSUAL	DESCRIPCIÓN
CNT EP	$1.097,60	20 MBPS IPv6
LACNIC	$175,00	*POOL* /32 (Categoría Small)
TOTAL	$1.272,60	VALOR MENSUAL

Para poder llevar a cabo este proceso, se requiere contemplar, que la inversión en cuanto a capacitación del personal es la más costosa y además es la que demandará mayor tiempo.

Categoría	Prefijo Recursos IPv4	Prefijo Recursos IPv6	Inicial (USD)	Renovación (USD)	Pago antes del Vencimiento (*)	Pago pasado 30 días del vencimiento (**)
Small/Micro	Menor a /20	No existe	1.000	1.000	900	1.100
Small	Mayor o igual /20 hasta /19 inclusive	Hasta /32 inclusive	2.100	2.100	1.890	2.310
Medium	Mayor /19 y menor /16	Mayor /32 y menor /30	5.700	5.700	5.130	6.270
Large	Mayor o igual /16 y menor /14	Mayor o igual /30 y menor /28	14.000	14.000	12.600	15.400
Extra-Large	Mayor o igual /14 y menor /11	Mayor o igual /28 menor /26	28.000	28.000	25.200	30.800
Mayor	Mayor o igual /11	Mayor o igual /26	40.000	40.000	36.000	44.000

**De acuerdo al estatuto de LACNIC, los miembros Activos "A" tienen incluido en su cuota anual de renovación, el costo de la membresía.*

Figura 4.1 Tabla de Categoría y costos LACNIC *[33]*

El costo anual por la adjudicación de un bloque /32 por parte de LACNIC se detalla en la Figura 4.1. Para el caso del bloque solicitado, el costo inicial fue de $0,00 según la resolución de LACNIC en donde había una exoneración para todas las solicitudes realizadas hasta el 1 de julio de 2013 [34], la solicitud para Ecuaonline S.A. se la realizó el 30 de abril de 2013; el costo anual, por estar en una categoría Small, es de $2100,00 al año, lo que se traduce en un valor mensual de $175,00.

Con el estudio realizado, respecto diseño de la red de Ecuaonline S.A., se obtuvo una red que soportará los dos protocolos de red IPv4 e IPv6 en Doble Pila, para lo

cual, se decidió realizar algunos cambios en cuanto a equipos y proveedores. Este diseño plantea un costo estimado de $19.326,00 para poder trabajar con IPv6 en todos los segmentos de la red del proveedor, además se requiere realizar un pago mensual de $1.272,60 por el contrato de AB con CNT y la mensualidad a LACNIC por el *Pool* de direcciones IPv6.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

De los resultados técnico-económicos obtenidos, se pueden extraer las conclusiones siguientes:

5.1 CONCLUSIONES

- El número de direcciones IPv4 ha llegado a sus límites de asignación y utilización, presentado ya dificultades a los usuarios finales de obtener cada vez direccionamiento público para sus redes.
- Debido al auge de Internet que se ha vivido durante la última década, el espacio de direcciones IPv4 se ha ido agotando gradualmente. Ecuaonline S.A ante este problema, que amenaza el crecimiento de la Red de redes ha iniciado el estudio para la migración hacia IPv6.
- El espectacular crecimiento del tráfico en Internet y la tan ansiada convergencia de voz, datos e imagen en una única red, hacen necesaria la evolución de las comunicaciones que irían de la mano del protocolo IPv6.
- Ecuaonline S.A. ha iniciado la investigación en su red para implementar a futuro Doble Pila y así aumentar sus oportunidades de negocio. Con el estudio realizado, se puede entender de mejor manera lo que Ecuaonline S.A. necesita para poner en marcha la implementación del nuevo protocolo de Internet IPv6.
- En IPv4 las direcciones están compuestas por 4 bytes que equivalen a 32 bits teniéndose como direcciones IP posibles 2^{32}, es decir 4.294.967.296 de direcciones, mientras que con IPv6 se tiene un espacio de 16 bytes equivalentes a 128 bits. Lo que permitiría elevar la posibilidad de direcciones a 2^{128}, es decir 3.40282366921E38 de direcciones.
- Para la cantidad de usuarios que tiene Ecuaonline S.A, es un desperdicio de direcciones la asignación de un prefijo /32 que LACNIC asignó al proveedor. Según el estudio realizado, se comprueba que con un prefijo /37 es suficiente para cubrir las necesidades presentes y futuras.

- Se debe considerar que un prefijo /32 tiene 32 prefijos /37 por lo que se estará holgados de direcciones para muchísimos años.
- De forma general se puede decir que en los IGP no existe mayor cambio entre IPv4 e IPv6, de forma que si se conoce bien un protocolo de *routing* en IPv4, será fácil implementar su versión para IPv6. Esto se debe a que los protocolos de *routing* operan en el ámbito de aplicación o plano de control, y usan algoritmos independientes de la capa de red utilizada por lo que serán independientes de la versión de IP usada.
- Para soportar IPv6 se debe añadir al protocolo de enrutamiento la capacidad de enviar como *Next-Hop* una dirección IPv6, también de poder enviar información de prefijos IPv6 y por último comunicarse sobre IPv6, excepto IS-IS que ya se demostró que lo realiza directamente sobre la capa de enlace.
- Una vez que se aplique en la práctica se notará que se usa direcciones *Link-Local* como *Next-Hop* o para identificar a los *routers* vecinos, esto puede resultar molestoso al principio, pero se puede mejorar configurando manualmente las direcciones Link-Local, de forma que sean más entendibles o identificables por las personas.
- Al utilizar IPv6 en la red del proveedor, no es necesario pensar en aumentar el ancho de banda cuando se utilice el método de Doble Pila, ya que el tráfico de IPv4 será “robado” por el tráfico IPv6, es decir, que todo el contenido mostrado en Internet, se mostrará en un solo tipo de protocolo.
- IPv6 es un activador fundamental para la visión que se tiene de la sociedad de Información móvil. Actualmente, el número de teléfonos inalámbricos ya supera con creces el número de terminales fijos de Internet. En estos momentos, IPv6 se perfila como la única arquitectura viable que puede acomodar la nueva ola de dispositivos celulares capaces de soportar Internet.
- Una característica importante del protocolo IPv6 es su configuración *Plug and Play,* con lo cual la asignación de direcciones es dinámica, así los *hosts* pueden construir su propia dirección.
- La migración del protocolo IPv4 a IPv6 significa un cambio a nivel de backbone, Plataforma o Infraestructura para un ISP. Para el caso del

desarrollo de este proyecto en Ecuaonline S.A, se deberá cambiar en todos estos niveles.

- Se pudo comprobar que el grado de desarrollo actual del protocolo IPv6 permite sin mayores contratiempos la implementación de redes que funcionan únicamente sobre IPv6. El soporte IPv6 existente en los equipos de red permite prescindir totalmente de IPv4 para la totalidad de servicios que una red tradicionalmente ofrece. Incluso funciones avanzadas como MPLS, IPSec y Mobile IP ya cuentan con soporte oficial en redes IPv6.
- Los sistemas operativos y programas computacionales han demostrado también poseer un soporte IPv6 lo suficientemente maduro para permitir su uso en ambientes IPv6.
- La red IPv6 presentada en este proyecto constituye la base para futuros trabajos y actualizaciones de la red en pos de una integración total del protocolo en todos los equipos y servicios otorgados por la red de Ecuaonline S.A. El plan de direccionamiento IPv6 jerárquico desarrollado permite proveer de forma ordenada de direcciones IPv6 a todos los usuarios de la red de Ecuaonline S.A, dejando un gran espacio disponible para futuros clientes y servicios.
- Durante el presente proyecto se diseñó correctamente una red IPv6 operando en modalidad "*dual-stack*" sobre la red de Ecuaonline S.A. Se espera, puesto que se obtuvo el máximo cuidado para el diseño, que luego de la implementación, el rendimiento y comportamiento de Ecuaonline S.A. avale el diseño realizado.

De la experiencia adquirida durante la ejecución de este proyecto se pueden dar las recomendaciones siguientes:

5.2 RECOMENDACIONES

- Cuando se planee desplegar IPv6 en la red de Ecuaonline y en general, se recomienda empezar desde la red de *Core* y seguir hacia el cliente.

- Se deben hacer todas las pruebas necesarias dentro de un entorno de pruebas para que al desplegar IPv6, el Cliente no note problemas en su conexión.
- Para mejorar el transporte en la red de Ecuaonline S.A. se recomienda cambiar a futuro de red de distribución por MPLS que añadirá mayor disponibilidad del servicio al tratarse de un medio guiado.
- Antes de realizar la migración se debe considerar aspectos importantes que permitan diseñar un plan, teniendo en cuenta parámetros como el tamaño de la red, asignación de direcciones IPv6, actualización de equipos y sobre todo la seguridad y las herramientas que van a ser utilizadas para monitorear la red una vez la transición se ponga en marcha
- Se recomienda utilizar programas de gestión de direcciones llamadas IPAM (Administración de direcciones IP) [35] para tener una asignación ordenada de las direcciones IPv6.

REFERENCIAS BIBLIOGRÁFICAS

[1] «Wikipedia,» [En línea]. Disponible: https://es.wikipedia.org/wiki/Agotamiento_de_las_direcciones_IPv4.

[2] Wkipedia, «WIkipedia,» [En línea]. Disponible: https://es.wikipedia.org/wiki/Modelo_OSI. [Último acceso: 27 01 2016].

[3] Wikipedia, «Wikipedia,» [En línea]. Disponible: https://es.wikipedia.org/wiki/High-Level_Data_Link_Control. [Último acceso: 2016 01 28].

[4] Wikipedia, «Wikipedia,» [En línea]. Disponible: https://es.wikipedia.org/wiki/Frame_Relay. [Último acceso: 28 01 2016].

[5] Wikipedia, «Wikipedia,» [En línea]. Disponible: https://es.wikipedia.org/wiki/Point-to-Point_Protocol. [Último acceso: 28 01 2016].

[6] Wikipedia, «Wikipedia,» [En línea]. Disponible: https://es.wikipedia.org/wiki/Classless_Inter-Domain_Routing. [Último acceso: 28 01 2016].

[7] Caida, «Caida,» [En línea]. Disponible: http://www.caida.org/funding/nets-IPv6/nets-IPv6_proposal.xml. [Último acceso: 21 11 2015].

[8] Potaroo, «Potaroo,» [En línea]. Disponible: http://www.potaroo.net/tools/ipv4/. [Último acceso: 31 10 2015].

[9] LACNIC, «2.3.2.18.-Transferencias de bloques IPv4 dentro de la región LACNIC,» [En línea]. Disponible: http://www.lacnic.net/web/lacnic/manual-2. [Último acceso: 23 11 2015].

[10] Wikipedia. [En línea]. Disponible: http://wiki.nil.com/IPv6_EUI-64_interface_addressing. [Último acceso: 12 11 2015].

[11] Wikipedia, «Wikipedia,» [En línea]. Disponible: http://es.wikipedia.org/wiki/Intranet. [Último acceso: 12 11 2015].

[12] Google, «Google,» 14 11 2015. [En línea]. Disponible: https://www.google.com/intl/en/IPv6/statistics.html.

[13] Wiki, «Wireshark,» [En línea]. Disponible: https://wiki.wireshark.org/CLNP. [Último acceso: 28 01 2016].

[14] G. E, «Blogspot,» [En línea]. Disponible: http://ngrupoe.blogspot.com/2012/10/algoritmo-de-dijkstra-y-spf.html. [Último acceso: 28 01 2016].

[15] Wikipedia, «Wikipedia,» [En línea]. Disponible: https://en.wikipedia.org/wiki/Path_vector_protocol. [Último acceso: 28 01 2016].

[16] Wikitel. [En línea]. Disponible: http://wikitel.info/wiki/Radioenlace. [Último acceso: 21 10 2014].

[17] E. S.A, «Ecuaonline S.A,» [En línea]. Disponible: http://www.ecuaonline.net/. [Último acceso: 28 01 2016].

[18] Claro, «Claro,» [En línea]. Disponible: www.claro.com.ec/. [Último acceso: 12 12 2015].

[19] M. d. T. y. l. S. d. l. Informacion, «Ministerio de Telecomunicaciones y la Sociedad de la Informacion,» [En línea]. Disponible: http://www.telecomunicaciones.gob.ec/. [Último acceso: 28 01 2016].

[20] Cisco, «6labs Cisco,» [En línea]. Disponible: http://6lab.cisco.com/stats/cible.php?country=EC&option=all. [Último acceso: 25 11 2015].

[21] Lacnic, «Lacnic,» [En línea]. Disponible: www.lacnic.net/. [Último acceso: 28 12 2015].

[22] H. E. I. Services, «Hurricane Electric,» [En línea]. Disponible: http://bgp.he.net/country/EC. [Último acceso: 25 noviembre 2015].

[23] Brightcell, «Brightcell,» [En línea]. Disponible: http://www.brightcell.net/. [Último acceso: 28 12 2015].

[24] WiFidom, «WiFidom,» [En línea]. Disponible: http://www.WiFidom.com/fabricantes/allot/netenforcer/. [Último acceso: 28 12 2015].

[25] Bytecoders, «Bytecoders,» [En línea]. Disponible: http://bytecoders.net/content/netequalizer-para-pymes-y-mercado-wisp.html. [Último acceso: 28 12 2015].

[26] OGS, «OGS,» [En línea]. Disponible: http://www.ogs.ny.gov/purchase/prices/7701821350PL_Layer3.pdf. [Último acceso: 28 11 2015].

[27] NETEQUALIZER, «NETEQUALIZER,» [En línea]. Disponible: http://www.netequalizer.com/staffneteqpricelist.php. [Último acceso: 28 11 2015].

[28] S. EC, «SIGNAL EC,» [En línea]. Disponible: http://www.signal.ec/signal/index.php/component/virtuemart/mikrotik/sxt-lite5-detail?Itemid=0. [Último acceso: 29 11 2015].

[29] EPCOM, «EPCOM,» [En línea]. Disponible: http://www.epcom.net/product/A2E-ALTAI-TECHNOLOGIES-LTD-74399.html. [Último acceso: 28 11 2015].

[30] eBay, «eBay,» [En línea]. Disponible: http://www.amazon.com/Ubiquiti-AirMax-Titanium-Wireless-RM5-Ti/dp/B00BLTAG7G. [Último acceso: 28 11 2015].

[31] Ubnt, «Ubnt,» [En línea]. Disponible: https://www.ubnt.com/download. [Último acceso: 12 12 2015].

[32] Mikrotik, «Mikrotik,» [En línea]. Disponible: http://www.mikrotik.com/download. [Último acceso: 29 12 2015].

[33] LACNIC, «LACNIC,» [En línea]. Disponible: http://www.lacnic.net/web/lacnic/categoria-de-membresia. [Último acceso: 1 1 2016].

[34] LACNIC, «LACNIC,» [En línea]. Disponible: http://lacnic.net/documentos/lacnicxvii/asamblea/Propuesta_Asamblea_Exoneracion_de_pago_por_IPv6_ES.pdf. [Último acceso: 2013 5 1].

[35] Wikipedia, «Wikipedia,» [En línea]. Disponible: https://en.wikipedia.org/wiki/IP_address_management. [Último acceso: 12 01 2016].

[36] Wikipedia. [En línea]. Disponible: https://es.wikipedia.org/wiki/Enhanced_Interior_Gateway_Routing_Protocol. [Último acceso: 15 11 2015].

[37] Wikipedia. [En línea]. Disponible: https://es.wikipedia.org/wiki/Open_Shortest_Path_First. [Último acceso: 15 11 2015].

[38] Wikipedia. [En línea]. Disponible: https://es.wikipedia.org/wiki/IS-IS. [Último acceso: 15 11 2015].

[39] Wikipedia. [En línea]. Disponible: https://es.wikipedia.org/wiki/Border_Gateway_Protocol. [Último acceso: 15 11 2015].

[40] E. e. Cifras. [En línea]. Disponible: http://www.ecuadorencifras.gob.ec/proyecciones-poblacionales/. [Último acceso: 12 10 2015].

[41] CISCO, «CISCO,» 23 NOVIEMBRE 2015. [En línea]. Disponible: http://tools.cisco.com/ITDIT/CFN/jsp/SearchBySoftware.jsp.

[42] Ubiquiti, «ubiquiti,» 17 Julio 2015. [En línea]. Disponible: https://dl.ubnt.com/firmwares/XN-fw/v5.6.2/changelog.txt. [Último acceso: 28 noviembre 2015].

ANEXOS

ANEXO A

DISTRIBUCIÓN DE CLIENTES DE ECUAONLINE S.A.

La Tabla A-1 muestra los clientes de la ciudad de Quito

Tabla A-1 Clientes de la ciudad de Quito

NODO	CLIENTES	TIPO	NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
1			**NODO TWIN TOWERS**			
	1	*BUSINESS*	CREA COMUNICACIONES	Internet		CISCO 1711
	2	*BUSINESS*	MIGRACIÓN RELACIONES EXTERIORES	Internet		CISCO 1711
	3	*BUSINESS*	COMERCIO ITALIANA	Internet		CISCO 1711
	4	*BUSINESS*	PROLIFE	Internet		CISCO 1711
	5	*BUSINESS*	PENCAFLOR	Internet		CISCO 1711
	6	*BUSINESS*	COMDIGITRONIX	Internet		CISCO 1711
	7	*BUSINESS*	SNOB UIO (1/4)	Internet	Datos	CISCO 2610
	8	*BUSINESS*	VH COMUNICACIONES	Internet		CISCO 1711
	9	*BUSINESS*	BIOALIMENTAR QUITO (1/2)	Internet	Datos	CISCO 1711
	10	*BUSINESS*	ESTUDIO JURÍDICO NOBOA PEÑA Y LARREA	Internet		CISCO 1711
	11	*BUSINESS*	RAÚL REVELO (GALLERY ABOGADOS)	Internet		CISCO 1711
	12	*BUSINESS*	ECUANROSES ARCOIRIS (1/4)	Internet	Datos	CISCO 2610
	13	*BUSINESS*	RADISIS	Internet		CISCO 1711
	14	*BUSINESS*	DIRECCIÓN NACIONAL DE MIGRACIÓN	Internet		CISCO 1711
	15	*BUSINESS*	FIDU ECUADOR	Internet		CISCO 1711
	16	*BUSINESS*	ABP PUBLICIDAD	Internet		CISCO 1711
	17	*BUSINESS*	AMAZON	Internet		CISCO 1711
	18	*BUSINESS*	WORLD ECUADOR (WORLD MATRIZ)	Internet		CISCO 1711

NODO	CLIENTES	TIPO	NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
2			**NODO BUENOS AIRES**			
	1	BUSINESS	FLORES CELESTIALES	Internet		CISCO 1711
	2	*HOME*	SANTILLÁN BORJA FRANCISCO RAFAEL	Internet		D-LINK DIR 600
	3	BUSINESS	SEVILLA AMAYA VÍCTOR HUGO (LA HUERTA)	Internet		CISCO 1711
	4	BUSINESS	ARBUSTA FLORQUIN S.A. (1/4)	Internet	Datos	CISCO 2610
	5	BUSINESS	ECUAMERICA BRAZIL (1/2)	Internet	Datos	CISCO 1711
	6	BUSINESS	COMUMAP	Internet		CISCO 1711
	7	*HOME*	PAÚL AYALA	Internet		D-LINK DIR 600
	8	BUSINESS	COLEGIO AMÉRICA	Internet		CISCO 1711
	9	BUSINESS	PONY CENTRAL	Internet		CISCO 1711
	10	BUSINESS	INGE CABLE	Internet		CISCO 1711
	11	BUSINESS	LOGIANDINA S.A.	Internet		CISCO 1711
	12	BUSINESS	ELECTROBRAVER CIAL LTDA	Internet		CISCO 1711
	13	BUSINESS	ESCUELA JORGE ICAZA	Internet		CISCO 1711
	14	BUSINESS	INROSES 2 (1/3)	Internet	Datos	CISCO 1721
	15	BUSINESS	IMPRENTA MARISCAL	Internet		CISCO 1711
	16	BUSINESS	REMIGIO POZO - AGRIROSE	Internet		CISCO 1711
	17	BUSINESS	ARBUSTA (2/4)	Internet	Datos	CISCO 2610
	18	BUSINESS	NATIVE BLOOMS MONTESERRÍN	Internet		CISCO 1711
	19	BUSINESS	BROWNBREDING INGENIERÍA S.A.	Internet		CISCO 1711
	20	BUSINESS	MARÍA VALENTE (CAFENET MV)	Internet		CISCO 1711

NODO	CLIENTES	TIPO	NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
3			**NODO GONZÁLEZ SUÁREZ**			
	1	BUSINESS	PRODUNORTE GERENCIA (1/3)	Internet	Datos	CISCO 1721
	2	BUSINESS	GERENTE GALAPAGOS FLOWERS	Internet		CISCO 1711
	3	BUSINESS	SNOB PUEMBO (2/4)	Internet	Datos	CISCO 2610
	4	BUSINESS	LA ROSALEDA	Internet		CISCO 1711
	5	BUSINESS	FRAGMENTO HUMANO	Internet		CISCO 1711
	6	BUSINESS	FLORECC	Internet		CISCO 1711
	7	*HOME*	WILMA ESCALANTE	Internet		D-LINK DIR 600
	8	BUSINESS	ROSE ELITE RIESLINGFLOWER	Internet		CISCO 1711
	9	BUSINESS	VIAMERICA	Internet		CISCO 1711
	10	BUSINESS	PEÑA & NOBOA PANAVIAL PIFO	Internet		CISCO 1711
	11	BUSINESS	DEL CAMPO (LA HOLANDESA)	Internet		CISCO 1711
	12	BUSINESS	ALIANZA FRANCESA	Internet		CISCO 1711
	13	BUSINESS	VETFARM PIFO	Internet		CISCO 1711
	14	*HOME*	JUAN CARLOS PINEIDA	Internet		D-LINK DIR 600
	15	BUSINESS	ARBUSTA CUMBAYÁ (3/4)	Internet	Datos	CISCO 2610
	16	BUSINESS	COTA MATRIZ (1/2)	Internet	Datos	CISCO 1711
	17	*HOME*	MONSERRAT MEJÍA	Internet		D-LINK DIR 600
	18	BUSINESS	CASA HUMBOLDT	Internet		CISCO 1711
	19	BUSINESS	EXPOFLORES	Internet		CISCO 1711
	20	BUSINESS	PILONES LA VICTORIA	Internet		CISCO 1711

NODO	CLIENTES	TIPO	NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	21	BUSINESS	ECUAMERICA (2/2)	Internet	Datos	CISCO 1711
	22	BUSINESS	BRIGHTCELL MATRIZ	Internet		CISCO 2610
	23	BUSINESS	BACOLOGY ULLOA (1/3)	Internet	Datos	CISCO 1721
	24	BUSINESS	MATERIA GRIS	Internet		CISCO 1711
	25	BUSINESS	VENTURA MALL	Internet		CISCO 1711
4			**NODO ATUCUCHO**			
	1	BUSINESS	FERNANDO SAENZ OFICINA (1/2)	Internet	Datos	CISCO 1711
	2	BUSINESS	FERNANDO SAENZ CASA (2/2)	Internet	Datos	CISCO 1711
	3	BUSINESS	FLORES EXPRESS	Internet		CISCO 1711
	4	BUSINESS	BM PUBLICIDAD	Internet		CISCO 1711
	5	*HOME*	BELÉN CASARES	Internet		D-LINK DIR 600
	6	BUSINESS	RAFAEL POVEDA (COBERPACK)	Internet		CISCO 1711
	7	BUSINESS	SNOB (3/4)	Internet	Datos	CISCO 2610
	8	BUSINESS	COTA BODEGA (2/2)	Internet	Datos	CISCO 1711
	9	BUSINESS	FERROMEDICA	Internet		CISCO 1711
	10	BUSINESS	VEGAFLOR QUITO (1/3)	Internet	Datos	CISCO 1721
	11	BUSINESS	BANCOLOGY MATRIZ (2/3)	Internet	Datos	CISCO 1721
	12	BUSINESS	PYGANFLOR (COMITÉ DEL PUEBLO)	Internet		CISCO 1711
	13	*HOME*	VÍCTOR NAVARRO	Internet		D-LINK DIR 600
	14	BUSINESS	SJ YERSEY CENTRAL (1/3)	Internet	Datos	CISCO 1721
	15	BUSINESS	PATPRIMO MATRIZ (1/5)	Internet	Datos	CISCO 2610

NODO	CLIENTES	TIPO	NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	16	BUSINESS	SERVIA	Internet		CISCO 1711
5			**NODO SAN JUAN DE CALDERÓN**			
	1	BUSINESS	GALAFLOR QUINCHE (1/2)	Internet	Datos	CISCO 1711
	2	*HOME*	GERENTE SNOB	Internet		D-LINK DIR 600
	3	BUSINESS	COOPERATIVA DE AHORRO Y CRÉDITO SANTA ANA DE NAYÓN MATRIZ (1/3)	Internet	Datos	CISCO 1721
	4	BUSINESS	COOPERATIVA DE AHORRO Y CRÉDITO SANTA ANA DE NAYÓN GUALO (2/3)	Internet	Datos	CISCO 1721
	5	BUSINESS	COOPERATIVA DE AHOORO Y CRÉDITO SANTA ANA DE NAYÓN COMITÉ DEL PUEBLO (3/3)	Internet	Datos	CISCO 1721
	6	BUSINESS	PLASTIKYTO	Internet		CISCO 1711
	7	BUSINESS	SJ YERSEY CALDERÓN (2/3)	Internet	Datos	CISCO 1721
	8	BUSINESS	NEUMAN FLOWERS	Internet		CISCO 1711
	9	BUSINESS	ECUAFIORI EXPORT S.A	Internet		CISCO 1711
	10	BUSINESS	SANDE	Internet		CISCO 1711
	11	BUSINESS	PATPRIMO 2 (2/5)	Internet	Datos	CISCO 2610
	12	BUSINESS	VIOLETA FLOWERS	Internet		CISCO 1711
	13	*HOME*	HILSEA CHIVAN	Internet		D-LINK DIR 600
	14	*HOME*	MARCO CUEVA	Internet		D-LINK DIR 600
	15	*HOME*	JOSÉ LUIS GUAMÁN	Internet		D-LINK DIR 600
	16	BUSINESS	ALIMENTOS SUPERIOR PLANTA	Internet		CISCO 1711

NODO	CLIENTES	TIPO	NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	17	*HOME*	ELENA YAKLOVEVA	Internet		D-LINK DIR 600
	18	BUSINESS	FLORES DE LA COLONIA (FLODECOL2) (1/3)	Internet	Datos	CISCO 1721
	19	BUSINESS	HACIENDA VERDE	Internet		CISCO 1711
	20	BUSINESS	PIANGO FLOR S.A.	Internet		CISCO 1711
	21	BUSINESS	CAPSYD MALCHINGUI	Internet		CISCO 1711
	22	*HOME*	CARLOS MANTILLA	Internet		D-LINK DIR 600
	23	BUSINESS	HISLEA PERUCHO	Internet		CISCO 1711
	24	BUSINESS	COACSA LUMBISI	Internet		CISCO 1711
	25	BUSINESS	COLEGIO MALCHINGUI	Internet		CISCO 1711
	26	BUSINESS	JUNTA PARROQUIAL MALCHINGUI	Internet		CISCO 1711
6			**NODO COMITÉ DEL PUEBLO**			
	1	BUSINESS	IMBAUTO DISMARK (1/5)	Internet	Datos	CISCO 2610
	2	BUSINESS	ROOSVELT MONCAYO	Internet		CISCO 1711
7			**NODO PUENGASÍ**			
	1	*HOME*	IVÁN RUIZ	Internet		D-LINK DIR 600
	2	BUSINESS	INFLOWERS	Internet		CISCO 1711
	3	*HOME*	JAVI CORONEL	Internet		D-LINK DIR 600
	4	BUSINESS	INMOVILIARIA VERZAM (CARLOS VERA)	Internet		CISCO 1711
	5	BUSINESS	VVK ALIMENTOS	Internet		CISCO 1711
	6	BUSINESS	COLEGIO MONTEBELLO	Internet		CISCO 1711
	7	*HOME*	BASURTO CORNEJO NOELIA GENOVEVA	Internet		D-LINK DIR 600

NODO	CLIENTES	TIPO	NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	8	*HOME*	KEVIN VALLE	Internet		D-LINK DIR 600
	9	*HOME*	JUAN DIEGO ALMACHE	Internet		D-LINK DIR 600
	10	BUSINESS	PATPRIMO ECUADOR COMERCIALIZADORA S.A. (3/5)	Internet	Datos	CISCO 2610
	11	BUSINESS	HOSTERIA RANCHO DEL CIELO	Internet		CISCO 1711
	12	BUSINESS	ELIMED	Internet		CISCO 1711
	13	BUSINESS	UNIÓN VERA PLASTIK	Internet		CISCO 1711
	14	*HOME*	CARLOS LLUMIQUINGA	Internet		D-LINK DIR 600
8			**NODO MONJAS**			
	1	BUSINESS	FLOREQUISA (1/3)	Internet	Datos	CISCO 1721
9			**NODO PAQUISHA**			
	1	BUSINESS	ECOROSES	Internet		CISCO 1711
	2	BUSINESS	SNOB (4/4)	Internet	Datos	CISCO 2610
10			**NODO AMAGUAÑA**			
	1	BUSINESS	TEXTIL ECUADOR	Internet		CISCO 1711

La Tabla A-2 muestra los clientes de la ciudad de Latacunga

Tabla A-2 Clientes de la ciudad de Latacunga

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
1			**NODO QUILOTOA**			
	1	BUSINESS	ROSE SUCCESS	Internet		CISCO 1711
	2	*HOME*	CARLOS MARTINEZ	Internet		D-LINK DIR 600

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	3	BUSINESS	HOTEL JULIO SAN PEDRO	Internet		CISCO 1711
	4	*HOME*	CHANGOLUISA IZA ROSA MARÍA	Internet		D-LINK DIR 600
	5	*HOME*	MARÍA PILA	Internet		D-LINK DIR 600
	6	BUSINESS	EASTMANROSES CASA	Internet		CISCO 1711
	7	*HOME*	LUIS CHANCUSI	Internet		D-LINK DIR 600
	8	BUSINESS	HISPANO ROSE	Internet		CISCO 1711
	9	BUSINESS	UNIDAD EDUCATIVA FAE 5	Internet		CISCO 1711
	10	BUSINESS	CURTILAN	Internet		CISCO 1711
	11	BUSINESS	FUNDACIÓN SIERRA FLOR	Internet		CISCO 1711
	12	BUSINESS	ROSAS DEL COTOPAXI	Internet		CISCO 1711
	13	BUSINESS	FLORICOLA EASTMAN ROSES	Internet		CISCO 1711
	14	BUSINESS	ESCUELA DE PERFECCIONAMIENTO DE AEROTÉCNICOS	Internet		CISCO 1711
	15	BUSINESS	MARLEN ROSES (1/2)	Internet	Datos	CISCO 1711
	16	BUSINESS	ROSELY FLOWERS	Internet		CISCO 1711
	17	BUSINESS	LA CIENEGA	Internet		CISCO 1711
	18	*HOME*	RAMIRO MENA	Internet		D-LINK DIR 600
	19	BUSINESS	TOP ROSES	Internet		CISCO 1711
	20	BUSINESS	SIERRA FLOR (1/2)	Internet	Datos	CISCO 1711
	21	BUSINESS	AGRONPAXI	Internet		CISCO 1711
	22	*HOME*	CASA JULIO SAN PEDRO	Internet		D-LINK DIR 600

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	23	BUSINESS	RADIO OASIS	Internet		CISCO 1711
	24	*HOME*	JUAN CARLOS TOAPANTA	Internet		D-LINK DIR 600
	25	BUSINESS	COMPUWORLD 1	Internet		CISCO 1711
	26	*HOME*	KARINA GUANOLUISA	Internet		D-LINK DIR 600
2			**NODO GUANGO**			
	1	BUSINESS	ISINCHE FLOWERS	Internet		CISCO 1711
	2	*HOME*	NELLY VACA	Internet		D-LINK DIR 600
	3	*HOME*	RAÚL LEON	Internet		D-LINK DIR 600
	4	*HOME*	WASINGTON ACURIO	Internet		D-LINK DIR 600
	5	BUSINESS	AZERI FLOWERS	Internet		CISCO 1711
	6	BUSINESS	MERIZALDE	Internet		CISCO 1711
	7	BUSINESS	COLEGIO POALO	Internet		CISCO 1711
	8	*HOME*	GLORIA MARÍA PUCO	Internet		D-LINK DIR 600
	9	BUSINESS	MARLÉN ROSES 2 (2/2)	Internet	Datos	CISCO 1711
	10	BUSINESS	SANBEL FLOWERS	Internet		CISCO 1711
	11	BUSINESS	ACOLIT ASESORES Y CONSULTORES DEL LITORAL	Internet		CISCO 1711
	12	*HOME*	FERNANDO EASTMAN	Internet		D-LINK DIR 600
	13	BUSINESS	FLORES DE TOACAZO	Internet		CISCO 1711
	14	BUSINESS	HACIENDA TAMBO	Internet		CISCO 1711
	15	BUSINESS	PRESIDENCIA SIERRA FLOR	Internet		CISCO 1711

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	16	BUSINESS	INORFLOWERS	Internet		CISCO 1711
	17	BUSINESS	PILVICSA	Internet		CISCO 1711
	18	BUSINESS	LA ROSALEDA	Internet		CISCO 1711
	19	BUSINESS	ECUANROSES ARCOFLOR (2/4)	Internet	Datos	CISCO 2610
	20	BUSINESS	ECUANROSES MATRIZ (3/4)	Internet	Datos	CISCO 2610
	21	BUSINESS	ECUANROSES GROWERFARM (4/4)	Internet	Datos	CISCO 2610
	22	BUSINESS	SIERRA FLOR MATRIZ (2/2)	Internet	Datos	CISCO 1711
	23	BUSINESS	SPACIUM	Internet		CISCO 1711
	24	BUSINESS	LOCOAM FARMS	Internet		CISCO 1711
	25	BUSINESS	ESCUELA OSWALDO BONILLA	Internet		CISCO 1711
	26	BUSINESS	TAMBO 2 (2/2)	Internet	Datos	CISCO 1711
	27	BUSINESS	TAMBO 1 (1/2)	Internet	Datos	CISCO 1711
3			**NODO PILISURCO**			
	1	BUSINESS	BIOALIMENTAR (2/2)	Internet	Datos	CISCO 1711
	2	BUSINESS	INCUBANDINA	Internet		CISCO 1711
	3	BUSINESS	PAT PRIMO AMBATO (4/5)	Internet	Datos	CISCO 2610
	4	BUSINESS	BANCOLOGY (3/3)	Internet	Datos	CISCO 1721
	5	BUSINESS	YUYAK RUNA	Internet		CISCO 1711

La Tabla A-3 muestra los clientes de la ciudad de Ibarra

Tabla A-3 Clientes de la ciudad de Ibarra

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
1			**NODO IMANTAG**			
	1	BUSINESS	SACHS STEINHARDT BETTY JILL	Internet		CISCO 1711
	2	BUSINESS	MUSHUK PAKARY COTACACHI (1/3)	Internet	Datos	CISCO 1721
	3	BUSINESS	PAT PRIMO ATUNTAQUI (5/5)	Internet	Datos	CISCO 2610
	4	BUSINESS	DJNET	Internet		CISCO 1711
	5	BUSINESS	LA UNICA 2 (2/3)	Internet	Datos	CISCO 1721
	6	BUSINESS	INROSES COTACACHI (2/3)	Internet	Datos	CISCO 1721
	7	*HOME*	SOFIA BENAVIDES	Internet		D-LINK DIR 600
	8	BUSINESS	LA ÚNICA 1 (1/3)	Internet	Datos	CISCO 1721
	9	BUSINESS	PENCAFLOR	Internet		CISCO 1711
	10	BUSINESS	LA ÚNICA 3 (3/3)	Internet	Datos	CISCO 1721
	11	BUSINESS	SJ JERSEY (3/3)	Internet	Datos	CISCO 1721
	12	BUSINESS	RED ESCOLAR COTACACHI	Internet		CISCO 1711
	13	BUSINESS	MUSHUK PAKARI MATRIZ (2/3)	Internet	Datos	CISCO 1721
	14	BUSINESS	PLAZA NET	Internet		CISCO 1711
	15	BUSINESS	SOLNET	Internet		CISCO 1711
	16	*HOME*	PATRICIO RUIZ	Internet		D-LINK DIR 600
	17	*HOME*	JORGE DÁVILA	Internet		D-LINK DIR 600
2			**NODO IBARRA**			
	1	BUSINESS	SANTIAGO COLLAGUAZO (PUERTA VIRTUAL)	Internet		CISCO 1711

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	2	BUSINESS	FLORES DEL AMAZONAS	Internet		CISCO 1711
	3	BUSINESS	IMBAUTO GALPON (2/5)	Internet	Datos	CISCO 2610
	4	BUSINESS	IMBAUTO SOLO CHEVROLET (3/5)	Internet	Datos	CISCO 2610
	5	BUSINESS	IMBAUTO IBARRA (4/5)	Internet	Datos	CISCO 2610
	6	BUSINESS	MUSHUK IBARRA (3/3)	Internet	Datos	CISCO 1721
	7	BUSINESS	COMERCIAL HIDROBO MATRIZ (1/5)	Internet	Datos	CISCO 2610
	8	BUSINESS	COMERCIAL HIDROBO AUTHESA (2/5)	Internet	Datos	CISCO 2610
	9	BUSINESS	COMERCIAL HIDROBO MAZDA (3/5)	Internet	Datos	CISCO 2610
	10	BUSINESS	COMERCIAL HIDROBO PROINTEC (4/5)	Internet	Datos	CISCO 2610
	11	*HOME*	ADRIAN MERLO	Internet		D-LINK DIR 600
	12	*HOME*	PAVEL ESCALANTE	Internet		D-LINK DIR 600
	13	BUSINESS	RADIO IMPERIO FM (1/2)	Internet	Datos	CISCO 1711
	14	BUSINESS	RADIO IMPERIO AM (2/2)	Internet	Datos	CISCO 1711
	15	BUSINESS	CASA LUIS VITERI RADIO IMPERIO	Internet		CISCO 1711
	16	*HOME*	HECTOR PILATAXI	Internet		D-LINK DIR 600
	17	BUSINESS	HOTEL LA GIRALDA	Internet		CISCO 1711
	18	*HOME*	KATIA POZO	Internet		D-LINK DIR 600

La Tabla A-4 muestra los clientes de la ciudad de Otavalo

Tabla A-4 Clientes de la ciudad de Otavalo

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
1			**NODO COTAMA**			
	1	BUSINESS	COLEGIO TÉCNICO REPÚBLICA DEL ECUADOR	Internet		CISCO 1711
	2	*HOME*	PATRICIO SAAVEDRA	Internet		D-LINK DIR 600
	3	BUSINESS	NELLY PINEDA 2 (2/2)	Internet	Datos	CISCO 1711
	4	BUSINESS	NELLY PINEDA (1/2)	Internet	Datos	CISCO 1711
	5	BUSINESS	IMBAUTO OTAVALO (5/5)	Internet	Datos	CISCO 2610
	6	BUSINESS	HOSTAL MAY SHIS	Internet		CISCO 1711
	7	BUSINESS	INSTITUTO TÉCNICO OTAVALO	Internet		CISCO 1711
	8	*HOME*	ALEXIS MORA	Internet		D-LINK DIR 600
	9	BUSINESS	RED EDUCATIVA QUICHINCHE	Internet		CISCO 1711

La Tabla A-5 muestra los clientes de la ciudad de Cayambe

Tabla A-5 Clientes de la ciudad de Cayambe

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
1			**NODO SAN JOAQUÍN**			
	1	BUSINESS	NELLYS FLOWERS	Internet		CISCO 1711
	2	BUSINESS	FLOREQUISA (2/3)	Internet	Datos	CISCO 1721
	3	BUSINESS	FLOREQUISA VENTAS (3/3)	Internet	Datos	CISCO 1721
	4	BUSINESS	ARBUSTA (4/4)	Internet	Datos	CISCO 2610

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	5	BUSINESS	SAN BENITO	Internet		CISCO 1711
	6	BUSINESS	EXXIDE	Internet		CISCO 1711
	7	BUSINESS	INROSES (3/3)	Internet	Datos	CISCO 1721
	8	BUSINESS	LUXUSBLUMEN	Internet		CISCO 1711
	9	BUSINESS	PICASO FLOWERS	Internet		CISCO 1711
	10	*HOME*	HENRY SIERRA	Internet		D-LINK DIR 600
	11	BUSINESS	ECUAMADRIGAL	Internet		CISCO 1711
	12	BUSINESS	ANNIROSES	Internet		CISCO 1711
	13	BUSINESS	GALAFLOR (2/2)	Internet	Datos	CISCO 1711
	14	BUSINESS	CYBORNET	Internet		CISCO 1711
2			**NODO SILVERIO**			
	1	BUSINESS	FLODECOL (2/3)	Internet	Datos	CISCO 1721
	2	BUSINESS	FLORES DE LA COLINA (3/3)	Internet	Datos	CISCO 1721
	3	*HOME*	MANUEL BUITRÓN	Internet		D-LINK DIR 600
	4	BUSINESS	TURIS AGRONELPO	Internet		CISCO 1711
3			**NODO POROTOG**			
	1	BUSINESS	COMERCIAL HIDROBO (5/5)	Internet	Datos	CISCO 2610
	2	BUSINESS	MARUSROSES	Internet		CISCO 1711
	3	BUSINESS	DIRECCIÓN PROVINCIAL BILINGÜE	Internet		CISCO 1711
	4	BUSINESS	DIRECCIÓN PROVINCIAL AMBIENTE	Internet		CISCO 1711
	5	BUSINESS	EMAP PEDRO MONCAYO	Internet		CISCO 1711

NODO	CLIENTES		NOMBRES	SERVICIO 1	SERVICIO 2	EQUIPO
	6	BUSINESS	BRIHANNA	Internet		CISCO 1711
	7	*HOME*	JUAN CARLOS OBANDO	Internet		D-LINK DIR 600
	8	BUSINESS	JUNTA PARROQUIAL LA ESPERANZA	Internet		CISCO 1711
	9	BUSINESS	MYSTIC FLOWERS	Internet		CISCO 1711
	10	BUSINESS	FIORENTINA	Internet		CISCO 1711
	11	BUSINESS	ANNIROSES CASA	Internet		CISCO 1711
	12	BUSINESS	ROSADEX	Internet		CISCO 1711
	13	BUSINESS	JUNTA PARROQUIAL TOCACHI	Internet		CISCO 1711
	14	BUSINESS	FLOWERFEST	Internet		CISCO 1711
	15	BUSINESS	NELGOR	Internet		CISCO 1711
	16	BUSINESS	PRODUNORTE AGRONATURA (2/3)	Internet	Datos	CISCO 1721
	17	BUSINESS	AGRITAB 2	Internet		CISCO 1711
4			**NODO SANTA MÓNICA**			
	1	BUSINESS	HACIENDA GUACHALA	Internet		CISCO 1711
	2	BUSINESS	SANTA ANA	Internet		CISCO 1711
	3	BUSINESS	NÚCLEO DE FLORICULTORES	Internet		CISCO 1711
	4	*HOME*	MAURICIO TARANTO CEVALLOS	Internet		D-LINK DIR 600
	5	BUSINESS	RIOROSES	Internet		CISCO 1711
	6	BUSINESS	PRODUNORTE AYORA (3/3)	Internet	Datos	CISCO 1721
	7	BUSINESS	VEGA FLOR TUPIGACHI (2/3)	Internet	Datos	CISCO 1721
	8	BUSINESS	VEGA FLOR SAN PABLO (3/3)	Internet	Datos	CISCO 1721

ANEXO B

DIRECCIONAMIENTO IPv6

La Tabla B-1 muestra el rango de direcciones IPv6 para la Intranet

Tabla B-1 Rango de Direcciones IPv6 para la Intranet

#	*Networks (on nibble-boundary) (16 total)*	*IPv6.arpa addresses*
1	2803:0b00:0000:0000:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0000:0001:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0000:0002:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0000:0003:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:0000:0004:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
6	2803:0b00:0000:0005:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:0000:0006:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:0000:0007:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:0000:0008:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:0000:0009:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:0000:000a:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:0000:000b:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:0000:000c:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:0000:000d:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:0000:000e:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa
16	2803:0b00:0000:000f:0000:0000:0000:0000/64	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.0.0.0.0.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-2 muestra el rango de direcciones IPv6 disponibles para los usuarios Business + Datos

Tabla B-2 Rango de direcciones IPv6 disponibles para los usuarios Business + Datos

#	*Networks (on nibble-boundary) (64 total)*	*IPv6.arpa addresses*
1	2803:0b00:0040:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0041:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0042:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0043:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:0044:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
6	2803:0b00:0045:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:0046:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:0047:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:0048:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:0049:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:004a:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:004b:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:004c:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:004d:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:004e:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
16	2803:0b00:004f:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.4.0.0.0.0.b.0.3.0.8.2.ip6.arpa
17	2803:0b00:0050:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
18	2803:0b00:0051:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
19	2803:0b00:0052:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
20	2803:0b00:0053:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
21	2803:0b00:0054:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (64 total)*	*IPv6.arpa addresses*
22	2803:0b00:0055:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
23	2803:0b00:0056:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
24	2803:0b00:0057:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
25	2803:0b00:0058:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
26	2803:0b00:0059:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
27	2803:0b00:005a:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
28	2803:0b00:005b:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
29	2803:0b00:005c:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
30	2803:0b00:005d:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
31	2803:0b00:005e:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
32	2803:0b00:005f:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.5.0.0.0.0.b.0.3.0.8.2.ip6.arpa
33	2803:0b00:0060:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
34	2803:0b00:0061:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
35	2803:0b00:0062:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
36	2803:0b00:0063:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
37	2803:0b00:0064:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
38	2803:0b00:0065:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
39	2803:0b00:0066:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
40	2803:0b00:0067:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
41	2803:0b00:0068:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
42	2803:0b00:0069:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
43	2803:0b00:006a:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
44	2803:0b00:006b:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (64 total)*	*IPv6.arpa addresses*
45	2803:0b00:006c:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
46	2803:0b00:006d:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
47	2803:0b00:006e:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
48	2803:0b00:006f:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.6.0.0.0.0.b.0.3.0.8.2.ip6.arpa
49	2803:0b00:0070:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
50	2803:0b00:0071:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
51	2803:0b00:0072:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
52	2803:0b00:0073:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
53	2803:0b00:0074:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
54	2803:0b00:0075:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
55	2803:0b00:0076:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
56	2803:0b00:0077:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
57	2803:0b00:0078:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
58	2803:0b00:0079:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
59	2803:0b00:007a:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
60	2803:0b00:007b:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
61	2803:0b00:007c:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
62	2803:0b00:007d:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
63	2803:0b00:007e:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa
64	2803:0b00:007f:0000:0000:0000:0000:0000/48	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.7.0.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-3 muestra el rango de direcciones IPv6 disponibles para los usuarios Business de Quito

Tabla B-3 Rango de direcciones IPv6 disponibles para los usuarios Business de Quito

#	*Networks (on nibble-boundary) (128 total)*	*IPv6.arpa addresses*
1	2803:0b00:05f8:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:05f8:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:05f8:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:05f8:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:05f8:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
6	2803:0b00:05f8:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:05f8:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:05f8:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:05f8:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:05f8:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:05f8:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:05f8:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:05f8:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:05f8:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:05f8:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
16	2803:0b00:05f8:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.8.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
17	2803:0b00:05f9:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
18	2803:0b00:05f9:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
19	2803:0b00:05f9:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
20	2803:0b00:05f9:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
21	2803:0b00:05f9:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
22	2803:0b00:05f9:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (128 total)*	*IPv6.arpa addresses*
23	2803:0b00:05f9:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
24	2803:0b00:05f9:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
25	2803:0b00:05f9:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
26	2803:0b00:05f9:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
27	2803:0b00:05f9:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
28	2803:0b00:05f9:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
29	2803:0b00:05f9:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
30	2803:0b00:05f9:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
31	2803:0b00:05f9:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
32	2803:0b00:05f9:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.9.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
33	2803:0b00:05fa:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
34	2803:0b00:05fa:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
35	2803:0b00:05fa:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
36	2803:0b00:05fa:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
37	2803:0b00:05fa:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
38	2803:0b00:05fa:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
39	2803:0b00:05fa:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
40	2803:0b00:05fa:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
41	2803:0b00:05fa:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
42	2803:0b00:05fa:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
43	2803:0b00:05fa:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
44	2803:0b00:05fa:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
45	2803:0b00:05fa:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (128 total)*	*IPv6.arpa addresses*
46	2803:0b00:05fa:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
47	2803:0b00:05fa:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
48	2803:0b00:05fa:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.a.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
49	2803:0b00:05fb:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
50	2803:0b00:05fb:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
51	2803:0b00:05fb:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
52	2803:0b00:05fb:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
53	2803:0b00:05fb:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
54	2803:0b00:05fb:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
55	2803:0b00:05fb:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
56	2803:0b00:05fb:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
57	2803:0b00:05fb:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
58	2803:0b00:05fb:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
59	2803:0b00:05fb:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
60	2803:0b00:05fb:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
61	2803:0b00:05fb:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
62	2803:0b00:05fb:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
63	2803:0b00:05fb:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
64	2803:0b00:05fb:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.b.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
65	2803:0b00:05fc:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
66	2803:0b00:05fc:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
67	2803:0b00:05fc:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
68	2803:0b00:05fc:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (128 total)*	*IPv6.arpa addresses*
69	2803:0b00:05fc:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
70	2803:0b00:05fc:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
71	2803:0b00:05fc:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
72	2803:0b00:05fc:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
73	2803:0b00:05fc:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
74	2803:0b00:05fc:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
75	2803:0b00:05fc:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
76	2803:0b00:05fc:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
77	2803:0b00:05fc:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
78	2803:0b00:05fc:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
79	2803:0b00:05fc:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
80	2803:0b00:05fc:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.c.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
81	2803:0b00:05fd:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
82	2803:0b00:05fd:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
83	2803:0b00:05fd:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
84	2803:0b00:05fd:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
85	2803:0b00:05fd:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
86	2803:0b00:05fd:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
87	2803:0b00:05fd:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
88	2803:0b00:05fd:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
89	2803:0b00:05fd:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
90	2803:0b00:05fd:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
91	2803:0b00:05fd:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (128 total)*	*IPv6.arpa addresses*
92	2803:0b00:05fd:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
93	2803:0b00:05fd:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
94	2803:0b00:05fd:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
95	2803:0b00:05fd:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
96	2803:0b00:05fd:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.d.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
97	2803:0b00:05fe:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
98	2803:0b00:05fe:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
99	2803:0b00:05fe:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
100	2803:0b00:05fe:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
101	2803:0b00:05fe:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
102	2803:0b00:05fe:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
103	2803:0b00:05fe:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
104	2803:0b00:05fe:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
105	2803:0b00:05fe:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
106	2803:0b00:05fe:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
107	2803:0b00:05fe:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
108	2803:0b00:05fe:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
109	2803:0b00:05fe:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
110	2803:0b00:05fe:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
111	2803:0b00:05fe:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
112	2803:0b00:05fe:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.e.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
113	2803:0b00:05ff:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
114	2803:0b00:05ff:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (128 total)*	*IPv6.arpa addresses*
115	2803:0b00:05ff:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
116	2803:0b00:05ff:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
117	2803:0b00:05ff:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
118	2803:0b00:05ff:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
119	2803:0b00:05ff:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
120	2803:0b00:05ff:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
121	2803:0b00:05ff:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
122	2803:0b00:05ff:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
123	2803:0b00:05ff:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
124	2803:0b00:05ff:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
125	2803:0b00:05ff:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
126	2803:0b00:05ff:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
127	2803:0b00:05ff:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa
128	2803:0b00:05ff:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.f.5.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-4 muestra el rango de direcciones IPv6 disponibles para los usuarios Home de Quito.

Tabla B-4 Rango de direcciones IPv6 disponibles para los usuarios Home de Quito

#	*Networks (on nibble-boundary) (32 total)*	*IPv6.arpa addresses*
1	2803:0b00:0400:0000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0400:0100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0400:0200:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0400:0300:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:0400:0400:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (32 total)*	*IPv6.arpa addresses*
6	2803:0b00:0400:0500:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:0400:0600:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:0400:0700:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:0400:0800:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:0400:0900:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:0400:0a00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:0400:0b00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:0400:0c00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:0400:0d00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:0400:0e00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
16	2803:0b00:0400:0f00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.0.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
17	2803:0b00:0400:1000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
18	2803:0b00:0400:1100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
19	2803:0b00:0400:1200:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
20	2803:0b00:0400:1300:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
21	2803:0b00:0400:1400:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
22	2803:0b00:0400:1500:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
23	2803:0b00:0400:1600:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
24	2803:0b00:0400:1700:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
25	2803:0b00:0400:1800:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
26	2803:0b00:0400:1900:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
27	2803:0b00:0400:1a00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
28	2803:0b00:0400:1b00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (32 total)*	*IPv6.arpa addresses*
29	2803:0b00:0400:1c00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
30	2803:0b00:0400:1d00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
31	2803:0b00:0400:1e00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa
32	2803:0b00:0400:1f00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.1.0.0.4.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-5 muestra el rango de direcciones IPv6 disponibles para los usuarios Business de Latacunga.

Tabla B-5 Rango de direcciones IPv6 disponibles para los usuarios Business de Latacunga

#	*Networks (on nibble-boundary) (64 total)*	*IPv6.arpa addresses*
1	2803:0b00:001c:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:001c:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:001c:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:001c:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:001c:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
6	2803:0b00:001c:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:001c:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:001c:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:001c:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:001c:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:001c:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:001c:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:001c:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:001c:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:001c:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.c.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (64 total)*	*IPv6.arpa addresses*
16	2803:0b00:001c:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.c.1.0.0.0.b.0.3.0.8.2.ip6.arpa
17	2803:0b00:001d:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
18	2803:0b00:001d:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
19	2803:0b00:001d:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
20	2803:0b00:001d:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
21	2803:0b00:001d:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
22	2803:0b00:001d:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
23	2803:0b00:001d:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
24	2803:0b00:001d:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
25	2803:0b00:001d:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
26	2803:0b00:001d:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
27	2803:0b00:001d:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
28	2803:0b00:001d:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
29	2803:0b00:001d:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
30	2803:0b00:001d:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
31	2803:0b00:001d:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
32	2803:0b00:001d:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.d.1.0.0.0.b.0.3.0.8.2.ip6.arpa
33	2803:0b00:001e:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
34	2803:0b00:001e:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
35	2803:0b00:001e:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
36	2803:0b00:001e:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
37	2803:0b00:001e:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
38	2803:0b00:001e:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (64 total)*	*IPv6.arpa addresses*
39	2803:0b00:001e:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
40	2803:0b00:001e:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
41	2803:0b00:001e:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
42	2803:0b00:001e:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
43	2803:0b00:001e:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
44	2803:0b00:001e:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
45	2803:0b00:001e:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
46	2803:0b00:001e:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
47	2803:0b00:001e:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
48	2803:0b00:001e:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.e.1.0.0.0.b.0.3.0.8.2.ip6.arpa
49	2803:0b00:001f:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
50	2803:0b00:001f:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
51	2803:0b00:001f:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
52	2803:0b00:001f:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
53	2803:0b00:001f:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
54	2803:0b00:001f:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
55	2803:0b00:001f:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
56	2803:0b00:001f:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
57	2803:0b00:001f:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
58	2803:0b00:001f:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
59	2803:0b00:001f:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
60	2803:0b00:001f:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa
61	2803:0b00:001f:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.f.1.0.0.0.b.0.3.0.8.2.ip6.arpa

#	Networks (on nibble-boundary) (64 total)	IPv6.arpa addresses
62	2803:0b00:001f:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.f.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
63	2803:0b00:001f:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.f.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
64	2803:0b00:001f:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.f.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-6 muestra el rango de direcciones IPv6 disponibles para los usuarios Home de Latacunga.

Tabla B-6 Rango de direcciones IPv6 disponibles para los usuarios Home de Latacunga

#	Networks (on nibble-boundary) (16 total)	IPv6.arpa addresses
1	2803:0b00:0018:0000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0018:0100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0018:0200:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0018:0300:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:0018:0400:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
6	2803:0b00:0018:0500:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:0018:0600:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:0018:0700:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:0018:0800:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:0018:0900:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:0018:0a00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:0018:0b00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:0018:0c00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:0018:0d00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:0018:0e00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
16	2803:0b00:0018:0f00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.0.8.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-7 muestra el rango de direcciones IPv6 disponibles para los usuarios Business de Ibarra

Tabla B-7 Rango de direcciones IPv6 disponibles para los usuarios Business de Ibarra

#	*Networks (on nibble-boundary) (16 total)*	*IPv6.arpa addresses*
1	2803:0b00:0011:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0011:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0011:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0011:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:0011:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
6	2803:0b00:0011:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:0011:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:0011:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:0011:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:0011:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:0011:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:0011:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:0011:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:0011:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:0011:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa
16	2803:0b00:0011:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.1.1.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-8 muestra el rango de direcciones IPv6 disponibles para los usuarios Home de Ibarra

Tabla B-8 Rango de direcciones IPv6 disponibles para los usuarios Home de Ibarra

#	Networks (on nibble-boundary) (16 total)	IPv6.arpa addresses
1	2803:0b00:0010:0000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0010:0100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0010:0200:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0010:0300:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:0010:0400:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
6	2803:0b00:0010:0500:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:0010:0600:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:0010:0700:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:0010:0800:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:0010:0900:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:0010:0a00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:0010:0b00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:0010:0c00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:0010:0d00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:0010:0e00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa
16	2803:0b00:0010:0f00:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.0.0.1.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-9 muestra el rango de direcciones IPv6 disponibles para los usuarios Business de Otavalo

Tabla B-9 Rango de direcciones IPv6 disponibles para los usuarios Business de Otavalo

#	*Networks (on nibble-boundary) (16 total)*	*IPv6.arpa addresses*
1	2803:0b00:0013:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.1.0.0.0.b.0.3.0.8.2.ip6.arpa

2	2803:0b00:0013:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0013:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0013:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:0013:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
6	2803:0b00:0013:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:0013:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:0013:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:0013:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:0013:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:0013:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:0013:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:0013:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:0013:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:0013:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
16	2803:0b00:0013:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.3.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-10 muestra el Rango de direcciones IPv6 disponibles para los usuarios Businees de Cayambe

Tabla B-10 Rango de direcciones IPv6 disponibles para los usuarios Businees de Cayambe

#	*Networks (on nibble-boundary) (32 total)*	*IPv6.arpa addresses*
1	2803:0b00:0016:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0016:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.6.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0016:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.6.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0016:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.6.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:0016:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.6.1.0.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (32 total)*	*IPv6.arpa addresses*
6	2803:0b00:0016:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:0016:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:0016:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
9	2803:0b00:0016:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
10	2803:0b00:0016:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
11	2803:0b00:0016:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
12	2803:0b00:0016:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
13	2803:0b00:0016:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
14	2803:0b00:0016:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
15	2803:0b00:0016:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
16	2803:0b00:0016:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.6.1.0.0.0.b.0.3.0.8.2.ip6.arpa
17	2803:0b00:0017:0000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
18	2803:0b00:0017:1000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
19	2803:0b00:0017:2000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
20	2803:0b00:0017:3000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
21	2803:0b00:0017:4000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
22	2803:0b00:0017:5000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
23	2803:0b00:0017:6000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
24	2803:0b00:0017:7000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
25	2803:0b00:0017:8000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
26	2803:0b00:0017:9000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.9.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
27	2803:0b00:0017:a000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.a.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
28	2803:0b00:0017:b000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa

#	*Networks (on nibble-boundary) (32 total)*	*IPv6.arpa addresses*
29	2803:0b00:0017:c000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.c.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
30	2803:0b00:0017:d000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.d.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
31	2803:0b00:0017:e000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.e.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa
32	2803:0b00:0017:f000:0000:0000:0000:0000/52	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.f.7.1.0.0.0.b.0.3.0.8.2.ip6.arpa

La Tabla B-11 muestra el rango de direcciones IPv6 disponibles para los usuarios Home de Cayambe

Tabla B-11 Rango de direcciones IPv6 disponibles para los usuarios Home de Cayambe

#	Networks (on nibble-boundary) (8 total)	IPv6.arpa addresses
1	2803:0b00:0014:0000:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.1.0.0.0.b.0.3.0.8.2.ip6.arpa
2	2803:0b00:0014:0100:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.0.4.1.0.0.0.b.0.3.0.8.2.ip6.arpa
3	2803:0b00:0014:0200:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.2.0.4.1.0.0.0.b.0.3.0.8.2.ip6.arpa
4	2803:0b00:0014:0300:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.3.0.4.1.0.0.0.b.0.3.0.8.2.ip6.arpa
5	2803:0b00:0014:0400:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.0.4.1.0.0.0.b.0.3.0.8.2.ip6.arpa
6	2803:0b00:0014:0500:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.5.0.4.1.0.0.0.b.0.3.0.8.2.ip6.arpa
7	2803:0b00:0014:0600:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.6.0.4.1.0.0.0.b.0.3.0.8.2.ip6.arpa
8	2803:0b00:0014:0700:0000:0000:0000:0000/56	0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.7.0.4.1.0.0.0.b.0.3.0.8.2.ip6.arpa

ANEXO C

PROFORMAS PROVEEDORES

IPv6

La Figura C-1 muestra la cotización del proveedor CNT

Formato Versión:	001 - 2012

Fecha:	26/11/2015
Cotización No.:	
Cliente:	ECUAONLINE
Contacto:	Gabriel Andrés Bonilla
Teléfono:	099-3564528
E-Mail:	g.bonilla@ecuaonline.com

PROPUESTA COMERCIAL

DIRECCION LOCALIDAD A (Ciudad, ubicación, teléfono, etc.)	DIRECCION LOCALIDAD B (Ciudad, ubicación, teléfono, etc.)	SERVICIO	MEDIO DE ACCESO	DISPONIBILIDAD	CAPACIDAD	CARGO ÚNICO DE INSCRIPCIÓN E INSTALACIÓN (USD)	RENTA MENSUAL SERVICIO (USD)
CNT	ECUAONLINE S.A.	INTERNET IPv6	FIBRA	99.60%	20 Mbps	$ 300.00	$ 980.00

Observaciones: SUJETA A FACTIBILIDAD. LA TARIFA DE INSTALACIÓN PUEDE VARIAR DEPENDIENDO DEL RESULTADO DE LA FACTIBILIDAD TÉCNICA

	$ 300.00	$ 980.00
	$ 36.00	$ 117.60
	$ 336.00	$ 1,097.60

CONSIDERACIONES TÉCNICAS

Tiempo de implementación:	15 a 30 días luego de la firma de la documentación contractual. Cotización sujeta a revisión dependiendo de factibilidad técnica.
Soporte y monitoreo:	CNT E.P. garantiza soporte técnico 24x7, con niveles de escalamiento especificados en el SLA.
Disponibilidad del servicio:	Los acuerdos de nivel de servicio (SLA) se incluyen en el contrato, garantizando la calidad del enlace.
Propiedad de los equipos:	Los equipos terminales empleados para la prestación del servicio, los proveerá CNT E.P.

CONSIDERACIONES COMERCIALES

Impuestos	Los costos parciales (Sub-total Parcial) no incluyen impuestos.

Figura C-1 Cotización CNT

La Figura C-2 muestra la cotización del proveedor Telconet

R.U.C.: 0991327371001

COTIZACION

No. 002-011-000034829

NÚMERO DE AUTORIZACIÓN:

0111201315520409913273710010121100419

FECHA Y HORA DE AUTORIZACIÓN:

01/11/2013 15:52:04

AMBIENTE: Producción

EMISIÓN: Normal

CLAVE DE ACCESO:

1201301099132737100120020110000348290115511

TELCONET

Dir Matriz: Mz 109 Solar 21 Kennedy Norte

Dir Sucursal:

Contribuyente Especial Nro
OBLIGADO A LLEVAR CONTABILIDAD: SI

Razón Social / Nombres y Apellidos: ECUAONLINE S.A. RUC / CI: 1791774639001

Fecha Emisión: 01/11/2015 Guía Remisión:

Cod. Principal	Cod. Auxiliar	Cant	Descripción	Detalle Adicional	Detalle Adicional	Precio Unitario	Descuento	Precio Total
SISCTN		1	Internet Dedicado IPv6 20480kbps	Disponibilidad 99,5%		2100.00	0.00	2100.00
SSEG		1	INSTALACION			250.00	0.00	250.00
SISCTN								
GADM								

Información Adicional
Dirección:
Teléfono:
Email:

SUBTOTAL 12%	2350.00
SUBTOTAL 0%	
SUBTOTAL No Objeto IVA	
SUBTOTAL	2350.00
TOTAL Descuento	0.00
IVA 12%	282,00
ICE	
VALOR TOTAL	2632,00

Figura C-2 Cotización Telconet

La Figura C-3 muestra la cotización del proveedor Claro

Quito 27 de noviembre de 2015

Sr:
Gabriel Bonilla
Dpto. Técnico
Ecuaonline
Presente.-

PROFORMA PRODUCTOS

Reciba un cordial saludo de todos quienes hacemos **CLARO**

Nos es grato poner a vuestra consideración la gama más amplia en servicios de internet IPv6; con la mayor tecnología que hace de CLARO la empresa líder a nivel nacional y la primera marca más recordada en el Ecuador.

A continuación detallo el requerimiento solicitado por ustedes, para ser considerado:

IT	DES	Qty	P.Unitario	P.Total
1	Internet de 20 Mbps IPv6 Disponibilidad 99,54%	1	$1300,00	$1300,00
2	Instalación	1	$300,00	$300,00
			Suman	**$1.600,00**
			IVA	**$192,00**
			TOTAL	**$1.792,00**

Atentamente,

Byron García.
Asesor de Soluciones Empresariales

Asesores Empresariales
Celular: 593 93 9266630
Fijo: 593 2 500 4040 ext 1637

Figura C-3 Cotización Claro