UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

MODALIDAD ABIERTA Y A DISTANCIA

TEMA:

Diseño de la transición de direcciones IPv4 a IPv6 en la Extensión Universitaria de Zamora

Tesis de grado previa a la obtención del título de Ingeniería en Informática.

AUTORA:

Ghislayne Xiomara Vera Calva

DIRECTOR:

Ing. Rommel Vicente Torres Tandazo

CENTRO UNIVERSITARIO ZAMORA

2009

Ing. Rommel Vicente Torres Tandazo
DIRECTOR DE TESIS

C E R T I F I C A:

Que la Srta. Ghislayne Xiomara Vera Calva, autora de la tesis ***"Diseño de la transición de direcciones IPv4 a IPv6 en la Extensión Universitaria de Zamora"***, ha cumplido con los requisitos estipulados en el Reglamento General de la Universidad Técnica Particular de Loja, la misma que ha sido coordinada y revisada durante todo el proceso de desarrollo, desde su inicio hasta la culminación, por lo cual autorizo su presentación.

Zamora, junio del 2009

_____

Ing. Rommel Vicente Torres Tandazo
DIRECTOR DE TESIS

CESIÓN DE DERECHOS:

Yo, **Ghislayne Xiomara Vera Calva**, declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja, que en su parte pertinente textualmente dice: *"Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través o con el apoyo financiero, académico o institucional (operativo) de la Universidad"*.

_____

Ghislayne Xiomara Vera Calva

AUTORIA:

En el presente Proyecto de Tesis, todas las opiniones, criterios, conclusiones y recomendaciones vertidos en el presente informe de investigación son de absoluta responsabilidad de la autora.

Ghislayne Xiomara Vera Calva

DEDICATORIA:

Este trabajo de investigación lo dedico a DIOS por haberme permitido la culminación de una meta más en mi vida, permitiéndome adquirir muchos conocimientos en ésta prestigiosa Universidad, agradezco a mis padres por el apoyo prestado en estos cinco años de carrera universitaria y de manera especial dedico este trabajo a mi Novio quién ha sido un gran apoyo durante esta etapa de mi vida.

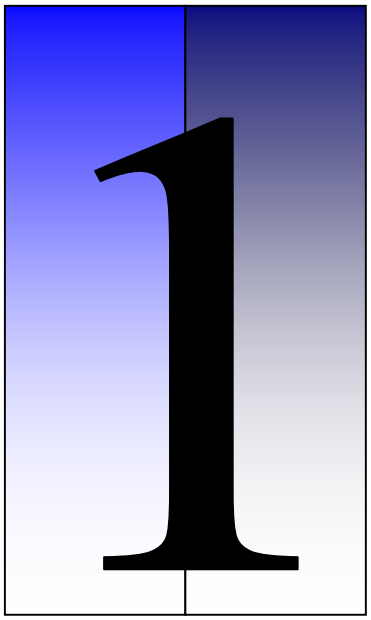
Ghislayne

AGRADECIMIENTO:

Mi sincero agradecimiento a la Universidad Técnica Particular de Loja, por haberme acogido y formado durante los cinco años de vida universitaria, al Ingeniero Rommel Torres director de mi tesis por su compresión y dedicación en la realización del presente Proyecto de Tesis y a todos quienes de una u otra manera contribuyeron en mi formación profesional.

Ghislayne

ÍNDICE DE CONTENIDOS



PERSPECTIVA ACTUAL DEL CAMBIO IPv4 A IPv6

Capítulo

1. INTRODUCCIÓN

La red de INTERNET utiliza los protocolos TCP/IP como normas y reglas básicas que administran eficientemente el tráfico de paquetes de datos que circula por la red mundial de información, los equipos conectados a internet se comunican utilizando direcciones IP, las cuales identifican tanto al ordenador como a la red a la que pertenecen. Actualmente la red de redes INTERNET está regida por la versión 4 del protocolo IP (IPv4), el uso de internet ha trascendido las expectativas previstas de crecimiento, convirtiéndose en la principal herramienta de envío y recepción de información; el aumento de usuarios, aplicaciones, servicios y dispositivos que requieren de una dirección IP nos están llevando a una nueva versión del protocolo IP.

Según las estadísticas presentadas por la página Internet World Stats. *[1]* Los últimos datos de usuarios conectados a internet para América Latina y el Caribe asciende a 139.009.209 usuarios, mientras que el porcentaje correspondiente al crecimiento de su uso entre los años 2000 - 2008 es de 669.3%, esta cifras nos permiten tener una idea clara del auge que ha tenido internet y con esto el inminente agotamiento de direcciones del actual protocolo lo cual nos lleva a buscar soluciones dando lugar a la versión sucesora del protocolo IP (IPv6).

IPv6 fue definido en la década del 90' por el Grupo de Trabajo en Ingeniería de Internet (IETF, del inglés Internet Engineering Task Force) y desde 1999 el IPv6 Forum preparó el despliegue de la nueva versión del protocolo IP versión 6 o IPng[1].*[2]* Esta revisión de las especificaciones actuales del protocolo IP ha sido motivada principalmente al hecho de que el sistema de direccionamiento (actualmente se utilizan 32 bits) se ha quedado limitado debido al gran auge de INTERNET, además el límite en el número de direcciones de red válidas está empezando a restringir el crecimiento de Internet y su uso.

[1] Internet Protocol Next Generation o "Siguiente Generación del Protocolo Internet"

En la actualidad el espacio de direcciones disponibles a nivel mundial del protocolo de red actual (IPv4), se ha reducido en su totalidad ya que IPv4 solamente cuenta con (4.000 millones de direcciones aproximadamente) con la intención de resolver este problema se desarrollaron algunos mecanismos o estrategias en IPv4 específicos, como por ejemplo el protocolo de Encaminamiento entre dominios sin clase (CIDR), la Traducción de dirección de red (NAT) y la Conmutación por etiquetas multiprotocolo (MPLS), pero éstos no cumplen con la necesidad de calidad de servicio en las comunicaciones punto a punto lo que ha impulsado el desarrollo de IPv6 que se muestra como la solución a los requerimientos actuales de direccionamiento.*[3]*

El Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC) es un organismo internacional sin fines de lucro, cuya función principal es la administración de los recursos de numeración de Internet asignados a América Latina y el Caribe. "Es un hecho que las direcciones IP basadas en la actual versión del protocolo (IPv4) se terminarán en corto plazo, se estima que en la actualidad queda disponible menos del 18% de total de las direcciones IP versión cuatro", dijo el Director Ejecutivo de LACNIC, Raúl Echeverría. LACNIC prepara campaña regional para incentivar la adaptación a la versión 6 del protocolo IP. *[4]*

La constante evolución y desarrollo de las tecnologías exige que la Universidad Técnica Particular de Loja, al constituir un Centro de Educación Superior de alta calidad ponga énfasis a la vanguardia tecnológica, es así que con la aparición de la versión 6 del protocolo IP se hace indispensable implementarlo en nuestra red académica ya que éste nos permitirá estar un paso delante lo cual se traduce en el ámbito educativo como desarrollo integral y que al contar con una Extensión Universitaria en la ciudad de Zamora, la misma que tiene el servicio de una Aula Virtual, la cual requiere la transferencia de videoconferencias en tiempo real con calidad de servicio, razón por la cual para mejorar éste servicio se plantea en el presente proyecto de tesis, la transición de direcciones de IPv4 a IPv6 para así poder tener una mayor Calidad de Servicio (QoS), Seguridad (IPSec) y Movilidad fundamentalmente, transferencia en tiempo real garantizada por el protocolo

de la nueva generación IPv6 como lo requiere la tecnología actual y como se lo merece esta entidad universitaria.

1.1 Protocolo IPv4[2]

Para dar respuesta a los problemas de capacidad de direccionamiento del protocolo IPv4 se adoptaron algunas soluciones como CIDR y NAT[3]:

De corto plazo/transitorias:

- **CIDR (Encaminamiento entre Dominios sin Clases):** Representa la última mejora en el modo como se interpretan las direcciones IP. Su introducción permite una mayor flexibilidad al dividir rangos de direcciones IP en redes separadas. CIDR engloba:
  - La técnica VLSM para especificar prefijos de red de longitud variable. Una dirección CIDR se escribe con un sufijo que indica el número de bits de longitud de prefijo, p.ej. 192.168.0.0/16 que indica que la máscara de red tiene 16 bits a uno. Esto permite un uso más eficiente del cada vez más escaso espacio de direcciones IPv4.
  - La agregación de múltiples prefijos contiguos en superredes, reduciendo el número de entradas en las tablas de ruta globales.
- **NAT (Traducción de Direcciones de Red):** Su uso más común es permitir utilizar direcciones privadas y aún así proveer conectividad con el resto de Internet. Si el número de direcciones privadas es muy grande puede usarse solo una parte de direcciones públicas para salir a Internet desde la red privada. De esta manera simultáneamente sólo pueden salir a Internet con una dirección IP tantos equipos como direcciones públicas se hayan contratado.

Definitivas:

IPv6: La ventaja del IPng respecto a la versión 4 del protocolo IP es evidente en cuanto a su capacidad de direccionamiento, debido a la

[2] RFC 791 - Protocolo Internet. Septiembre 1981

[3] No todos los routers soportan CIDR, además muchas aplicaciones requieren direcciones estáticas por lo que NAT no sirve de gran ayuda en IPv6.

inadecuada distribución de las direcciones del actual protocolo, las cuales se asignan en bloques regionales, registrándose una asignación excesiva en algunas zonas del mundo y un agotamiento de ellas en otras por ejemplo (Asia, Europa y América Latina). *[5]*

Cabecera del Protocolo IPv4:

El formato del protocolo IPv4 del encabezado que viaja actualmente en cada paquete de datos en internet, se muestra en la Tabla 1.

4	8	16	20	32
VERSIÓN	CABECERA	TOS	LONGITUD TOTAL	
IDENTIFICACION			INDICADOR	DESPLAZAMIENTO DEL FRAGMENTO
TTL (time to live)	PROTOCOLO		CHECKSUM	
DIRECCION ORIGEN 32 Bits				
DIRECCION DESTINO 32 Bits				
OPCIONES				

Campo modificado:	
Campo que desaparece:	

Tabla 1: Formato de la Cabecera del Protocolo IPv4

Direccionamiento IPv4:

En la versión 4 del protocolo IP (la usada actualmente) las direcciones están formadas por 4 números de 8 bits (un número de 8 bits en binario equivale en decimal desde 0 hasta 255) que se suelen representar separados por puntos, por ejemplo: **217.76.128.63** Cada dirección IP está conformada por 32 bits agrupados en 4 conjuntos de 8 bits cada uno (octetos). En la Figura 1 se presenta el formato de las direcciones del Protocolo IPv4.

Figura 1: Formato de las direcciones IPv4

Cada red de una empresa tiene una dirección; los hosts que residen en esa red comparten la misma dirección de red, pero cada host se identifica por medio de la dirección única de host en la red, es así que para apreciar de una forma clara se presenta en la Figura 2 el esquema en que se comunican las redes IPv4.

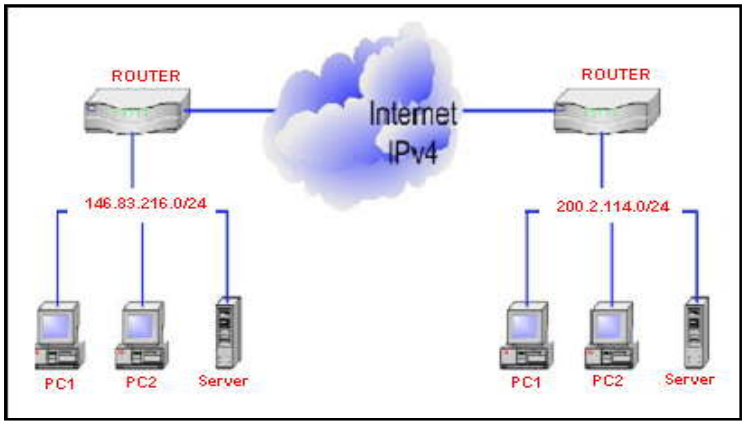


Figura 2: Esquema de comunicación en IPv4

Existen varios tipos de redes en el protocolo IPv4, las cuales se describen en la tabla 2.

CLASE	FORMATO				RANGO
A	RED	HOST	HOST	HOST	0.0.0.0 a 127.255.255.255
B	RED	RED	HOST	HOST	128.0.0.0 a 191.255.255.255
C	RED	RED	RED	HOST	192.0.0.0 a 223.255.255.255
D	ID GRUPO MULTICAST				224.0.0.0 a 239.255.255.255
E	EXPERIMENTAL				240.0.0.0 a 247.255.255.255

Tabla 2: Clases de direcciones en IPv4

1.2 Protocolo IPv6[4]

Algunos informáticos se preguntan ¿Porqué no IPv5?, estas direcciones fueron extensiones experimentales y no se acabaron de formalizarse en una nueva versión del protocolo, con lo que para evitar posibles

[4] RFC 2460 - Protocolo de Internet, versión 6 (IPv6). Diciembre 1998

conflictos de numeración y/o confusión, se optó por elegir el número de versión 6. *[6]*

Como se describe en la RFC 2460, IPv6 es el sustituto de IPv4. Aumenta el tamaño de las direcciones de IP de 32 a 128 bits, lo que da un total de 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones.

Este aumento en el espacio de direcciones no sólo proporciona mayor número de hosts, sino una jerarquía de direcciones mayor. Según "Christian Huitima (vocero del IETF) estima que habrá 1500 direcciones IPv6 por cada metro cuadrado de la superficie terrestre". *[7]*

Cabecera del Protocolo IPv6[5]**:**

El encabezado IPv6 ha pasando de 13 campos en IPv4 a únicamente 8, como se observa en la siguiente Tabla 3:

4	12	16	24	32
VERSIÓN	CLASE DE TRÁFICO	ETIQUETA DE FLUJO		
LONGITUD DE LA CARGA ÚTIL		SIGUIENTE CABECERA	LIMITE DE SALTOS	
DIRECCIÓN ORIGEN 128 Bits				
DIRECCIÓN DESTINO 128 Bits				

Tabla 3: Cabecera del Protocolo IPv6

En la lista siguiente se describe la función de cada campo del encabezado.

- **Versión**: número de versión de 4 bits del protocolo IP versión 6.
- **Clase de tráfico**: campo de clase de tráfico de 8 bits.
- **Etiqueta de flujo**: campo de 20 bits.
- **Tamaño de carga útil**: entero sin signo de 16 bits, que representa el resto del paquete que sigue al encabezado de IPv6, en octetos.
- **Encabezado siguiente**: selector de 8 bits. Identifica el tipo de encabezado que va inmediatamente después del encabezado de IPv6. Emplea los mismos valores que el campo de protocolo IPv4.

[5] RFC 3697 - Especificación del Protocolo Internet, versión 6 (IPv6). Marzo 2004

- **Límite de salto**: entero sin signo de 8 bits. Disminuye en uno cada nodo que reenvía el paquete. El paquete se desecha si el límite de salto se reduce a cero.
- **Dirección de origen**: 128 bits. Dirección del remitente inicial del paquete.
- **Dirección de destino**: 128 bits. Dirección del destinatario previsto del paquete. El destinatario previsto no es necesariamente el destinatario si existe un encabezado de encaminamiento opcional.

Se han mejorado las cabeceras de los paquetes, eliminando algunos campos de la cabecera de IPv4, haciendo que otros sean opcionales y utilizando cabeceras de extensión. Las cabeceras de extensión con cabeceras separadas que, con una excepción, no las examina ningún host en la ruta desde el origen hasta el destino, mejorando la eficiencia del enrutamiento. Además, permite una mayor flexibilidad en la codificación de opciones y capacidades de expansión para opciones futuras.

En IPv6 se introduce el etiquetado de flujos, lo que permite indicar que los paquetes pertenecen a determinado «flujo» de tráfico, de esta forma se permite manejar y la administración de ancho de banda sin tener que analizar cabeceras de TCP ni de UDP. También se han introducido extensiones que permiten autenticación, asegurar la integridad de los datos y cifrado de paquetes opcional. IPv6 incluye una terminología básica nueva, la cual se detalla en la Figura 3:

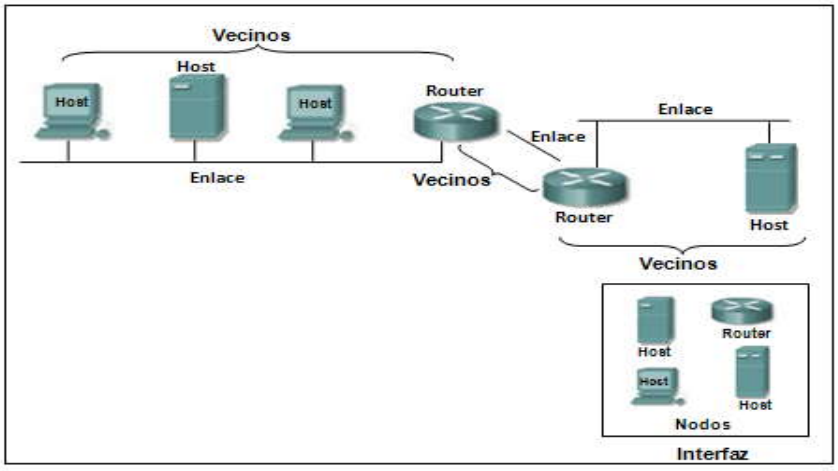


Figura 3: Terminología del direccionamiento IPv6

- **Nodos:** Un nodo es cualquier dispositivo con IPv6.
- **Enrutador:** Es un dispositivo que reenvía paquetes que no están directamente dirigidos a él.
- **Host:** Es un nodo que no reenvía paquetes.
- **Interfaz:** Una interfaz es la conexión con un medio de transmisión por la que se envían los paquetes de IPv6. Aunque se realice una distinción entre enrutadores y hosts, es posible, aunque poco probable, que un único nodo tenga varias interfaces y, potencialmente, reenvíe paquetes a direcciones de otros nodos o solamente a un subconjunto de sus interfaces. Es decir, este dispositivo actuaría como un host (en las interfaces que no reenvía) y como un enrutador (en las interfaces que reenvía).
- **Enlace:** Un enlace es el medio por el que se transporta IPv6.
- **Vecinos:** Los vecinos son nodos que están conectados al mismo enlace.
- **MTU del enlace:** Una unidad máxima de transmisión, MTU (Maximum Transmission Unit – Unidad Máxima de Transmisión) de un enlace es el tamaño máximo de paquete que se puede transportar por el medio del enlace, y se expresa en bytes.
- **Dirección del Nivel de enlace:** La dirección del Nivel de enlace es la dirección «física» de una interfaz, como la dirección de control de acceso al medio (MAC) en los enlaces Ethernet. En IPv6 todo el direccionamiento es a interfaces, no a los nodos.*[8]*

Direccionamiento IPv6[6]**:**

Las direcciones IPv6 son identificadores de 128 bits para interfaces y conjuntos de interfaces. Dichas direcciones se clasifican en tres tipos:

Unicast[7]**:** Identifica una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada por dicha dirección. El tipo de direccionamiento Unicast se muestra en la Figura 4.

[6] RFC 3513 Abordar la arquitectura IPv6. Abril 2003
[7] Unidifusión o punto a punto

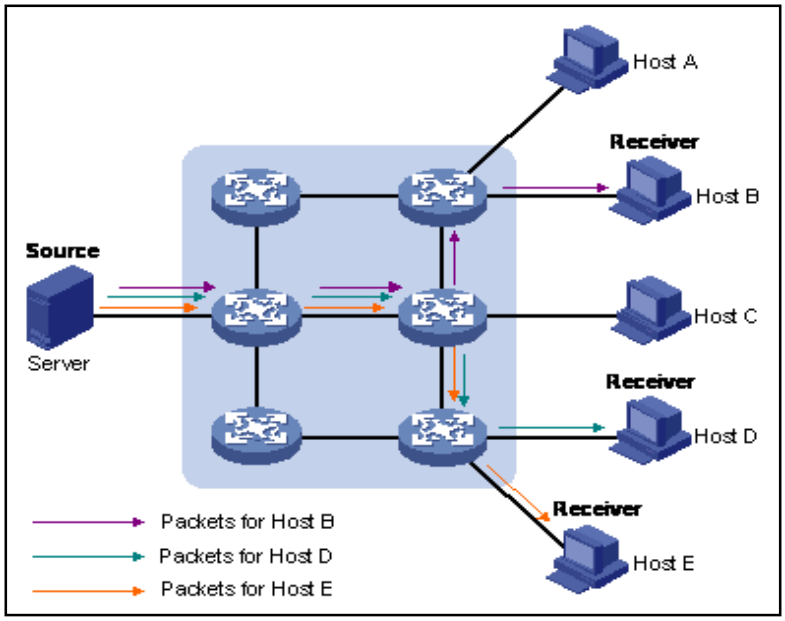
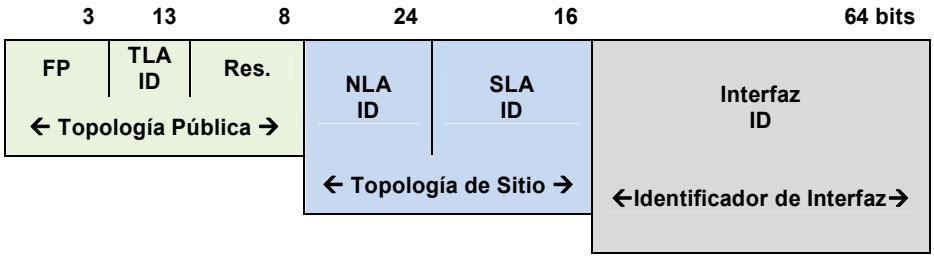


Figura 4: Direccionamiento Unicast IPv6

A continuación se describen los tipos de direcciones unicast de uso local:

- **Link-Local (Local de Enlace):** Se la utiliza para comunicaciones en el mismo enlace. Empiezan todas por ***fe80::***.Se crearon con propósitos de autoconfiguración, descubrimiento de vecinos (no atraviesan los routers).
- **Site-Local (Local de Sitio):** Para comunicaciones en el mismo sitio (pueden atravesar routers de un mismo sitio) para identificar interfaces en un mismo sitio. La definición de "sitio" es un tanto genérica, pero en principio un 'sitio' es el área topológica de red perteneciente a un edificio o un campus, perteneciente a una misma organización. Empiezan por ***fec0::***.
- **Global:** Para comunicaciones con servicios públicos. Estas direcciones se pueden utilizar en Internet y tienen el siguiente formato: 010(FP, 3 bits) TLA ID (13 bits) Reserved (8 bits) NLA ID (24 bits) SLA ID (16 bits) *idDeInterfaz* (64 bits). En la Tabla 4 se especifica los campos en una dirección Unicast global.



FP	Prefijo de Formato (001) Format – Prefix.
TLA ID	Identificador de Agregación de Nivel Superior -Top Level Aggregation Identifier.
Res.	Reservado para uso futuro.
NLA ID	Identificador de Agregación de Siguiente Nivel - Next Level Aggregation Identifier
SLA ID	Identificador de Agregación de Nivel de Sitio - Site Level Aggregation Identifier.
Interfaz ID	Identificador de Interfaz.

Tabla 4: Estructura de direcciones unicast globales

Multicast[8]**:** Identifica un conjunto de interfaces. Un paquete enviado a una dirección multicast[9] es entregado a todas las interfaces del conjunto identificadas con dicha dirección, el esquema del direccionamiento Multicast se presenta en la Figura 5.

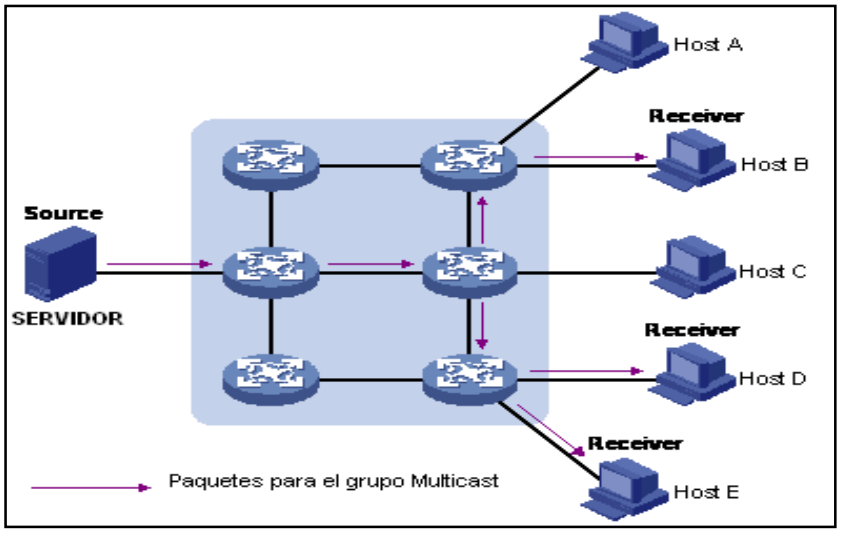


Figura 5: Direccionamiento Multicast IPv6

[8] Multidifusión o multi punto
[9] RFC 1112 - Anfitrión extensiones de IP multicasting. Agosto 1989

Anycast: Una dirección anycast, aunque identifica a varias interfaces, y normalmente a múltiples nodos, se envía sólo a la interfaz que es la más "cercana" al origen. El tráfico de paquetes con direcciones Anycast se observa en la Figura 6.

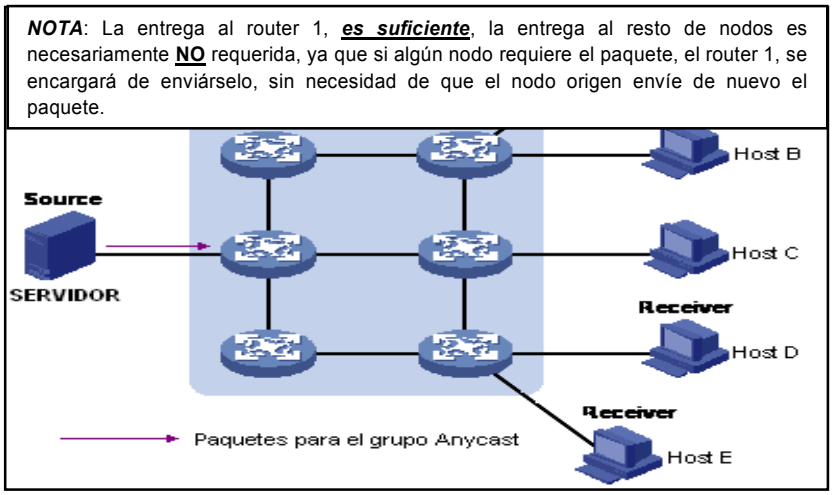


Figura 6: Direccionamiento Anycast IPv6

TIPO DE DIRECCIÓN	PREFIJO BINARIO
IPv4 compatible	000.0 (96 bits en 0)
Global unicast	001
Link-Local unicast	1111 1110 10
Site-Local unicast	1111 1110 11
Multicast	1111 1111

Tabla 5: Tipos de Prefijos

En la tabla 5 se hace referencia a los tipos de prefijos de acuerdo al tipo de dirección, a continuación se muestra las formas de representación de las direcciones IPv6.

Representación de Direcciones IPv6:

La Estructura de las direcciones IPv6 está compuesta por dos partes lógicas que son:

Prefijo: Depende de la topología de la red
Id. de Interfaz: Identifica a un nodo

La representación de direcciones IPv6 se realiza de tres formas:

- **Formato Preferido:**

  X:X:X:X:X:X:X:X (X = valores en hexadecimal de los ocho bloques de 16 bits de la dirección).

  Ejemplo:

  3ffe:3328:4:3:2:250:4ff:fe5c:b3f4
  Prefijo **Id. de Interfaz**

- **Formato comprimido:**

  Este método permite agrupar largas series de 0's, para hacer más legibles las direcciones, el uso de "::" indica múltiples grupos de 16 bits a 0.

  Ejemplos:

  1080:0:0:0:8:800:200C:417A podría representarse como
  1080::8:800:200C:417A
  FF01:0:0:0:0:0:0:43 podría representarse como FF01::43
  Sólo puede usarse "**::**" una vez en una dirección.

- **IPv4-compatible:**

  Este método resulta el más indicado para representar direcciones IPv6 que contengan direcciones IPv4, los 2 últimos bloques de 16 bits se representan como 4 bloques de 8 bits mostrando sus valores en decimal, como en IPv4.

  Ejemplos:

  0:0:0:0:0:0:13.1.68.3 ó ::13.1.68.3
  0:0:0:0:0:FFFF:129.144.52.38 ó ::FFFF:129.144.52.38. *[9]*

1.3 Principales diferencias entre IPv4 e IPv6

- **Mayor espacio de direcciones**: el tamaño de las direcciones IPv4 cambia de 32 bits a 128 bits, para soportar más niveles de jerarquías de direccionamiento y más nodos direccionales.
- **Simplificación del formato del Header**: algunos campos del Header IPv4 se eliminan o se hacen opcionales.
- **Paquetes IPv6 eficientes y extensibles**: sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesamiento por parte del router.
- **Posibilidad de paquetes con carga útil (datos)**: IPv6 tiene la capacidad de enviar paquetes de hasta 65.355 bytes.
- **Seguridad en el núcleo del protocolo (IPsec)[10]:** el soporte de IPsec es un requerimiento del protocolo IPv6.
- **Capacidad de etiquetas de flujo**: puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como la calidad de servicio o el servicio de tiempo real. Por ejemplo: las video conferencias.
- **Autoconfiguración:** la autoconfiguración de direcciones es más simple. Especialmente en direcciones Globales Unicast, los 64 bits superiores son asignados por un mensaje desde el router (Router Advertisement) y los 64 bits más bajos son asignados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.
- **Renumeración y "multihoming":** facilitando el cambio de proveedor de servicios.
- **Características de movilidad**: es la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.
- **Calidad de servicio (QoS)** y clase de servicio **(CoS).**

[10] IP Security Protocol o “Protocolo de Seguridad para Internet”.

- **Capacidades de autenticación y privacidad**. *[10]*

1.4 Características propias de IPv6:

- **Movilidad.-** IPv6 trae numerosas y significativas mejoras respecto a IPv4, uno de los aspectos en el que obtendremos importantes beneficios será la movilidad. En este sentido, cada vez más necesitamos que la comunicación pueda llevarse a acabo en cualquier momento y lugar con un óptimo grado de operatividad, así como de forma transparente al usuario realicen su propia gestión y control. Cuestiones de vital importancia si queremos disfrutar de servicios multimedia en los terminales móviles de última generación (VozIP y vídeo). Protocolos como MPI (Mobile IP) o HMIP (Hierarchical MIP) posibilitan la implantación y explotación real de estos servicios. Por este motivo, en IPv6 la movilidad es una funcionalidad obligatoria. *[11]*

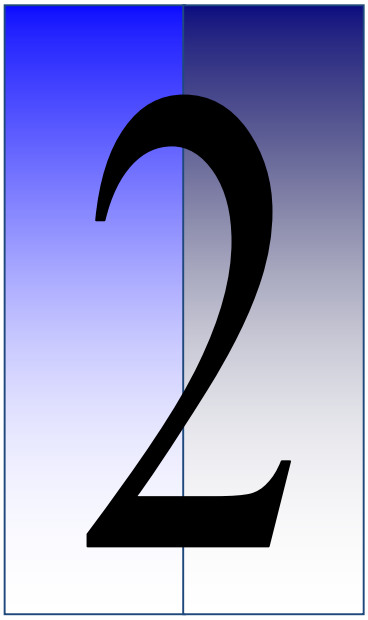
- **Seguridad.-** IPv6 proporciona total integración de los servicios de seguridad mediante dos mecanismos de seguridad: Autenticación de los paquetes, realizada con el Authentication Header.[11] El segundo mecanismo es el Payload Security Encriptación "End to End" del paquete realizada con el Encapsulating Security Payload Header[12] ofreciendo autenticación y confidencialidad (encriptación) dentro del núcleo del protocolo cumpliendo así con los requerimientos de seguridad de cada usuario en particular, es por ello que viene de manera obligatoria IPsec[13].

- **Extensibilidad de Direcciones**.- IPv6 incrementa el tamaño de las direcciones de 32 bits (IPv4) a 128 bits, para soportar más niveles en la jerarquía de direccionamiento, un número mayor de nodos direccionables, y un sistema de autoconfiguración de direcciones. Se añade un nuevo tipo de dirección, la llamada anycast, de forma que es posible enviar un paquete a cualquier nodo entre un grupo de ellos.

[11] RFC 2402 - Cabecera de Autenticación IP. Noviembre 1998
[12] RFC 2406 - Carga útil de Seguridad de Encapsulación de IP (ESP). Noviembre 1998
[13] RFC 2401 - Arquitectura de Seguridad para IP. Noviembre 1998

- **Calidad de Servicio (QoS).-** "Capacidad de una red para sostener un comportamiento adecuado del tráfico que transita por ella, cumpliendo con parámetros relevantes para el usuario final." IPv6 fue diseñado con un extendido soporte a QoS. En el encabezamiento se han incluido dos campos relacionados a QoS, estos son: Clase de tráfico e Identificador de Flujo.

- **Multihomming.-** IPv6 tiene la capacidad de realizar con facilidad el cambio de ISP´s, (Proveedores del Servicio de Internet) es decir si una empresa o institución de sea realizar el cambio de un proveedor a otro por varios motivos, no necesita cambiar de dirección, ni realizar una nueva configuración de los equipos, simplemente se acopla a los requerimientos de la configuración anterior.



Capítulo

MECANISMOS DE TRANSICIÓN

2. MECANISMOS DE TRANSICIÓN DE IPv4 A IPv6

La transición de IPv4 a IPv6 no es sencilla, por lo cual se la debe realizar de forma gradual mientras la coexistencia entre el protocolo actual y la versión seis es un hecho, tarde o temprano se tiene que producir un cambio de direcciones de 32 a 128 bits, sin afectar a los servicios que se prestan en la actualidad.

El primer paso hacia la transición es la instalación de equipos y aplicaciones que tengan capacidad para procesar los paquetes generados por ambos protocolos, por lo cual este proceso debe ir acompañado por un mecanismo que conjuntamente con los DNS *(*Domain Name System o Nombre de Dominio del Sistema*)*, transformen los dominios actuales en direcciones de 128 bits, a su vez esta debe ir acompañada de una política encaminada a guiar a los nuevos usuarios hacia la versión 6 del protocolo IP.

Hoy en día existen algunos mecanismos que permiten la coexistencia y la migración progresiva tanto de las redes como de los equipos de usuario. En general, los mecanismos de transición se clasifican en tres grupos:

- Dual Stack (Pila dual)
- Túneles
- Traducción

2.1 Dual Stack (Pila dual)

Este mecanismo es uno de los más comunes en los procesos de transición, los ruteadores trabajan y operan a doble pila simultáneamente en la misma infraestructura (IPv4+IPv6), un dispositivo con ambas pilas pueden recibir y enviar trafico a nodos que solo soportan uno de los dos protocolos.

2.1.1 Manual

Cuando el usuario conoce la dirección IPv6 del nodo destino. Para aplicaciones Web es necesario utilizar el formato para direcciones en un URL[14]. El uso de direcciones manuales solo es

[14] RFC 2732 – Formato de las direcciones IPv6 literales en la URL. Diciembre 1999

recomendable para propósitos de depuración, en lo posible debe utilizarse un servicio de nombres de dominio.

2.1.2 Utilizando un servicio de nombres de dominio

Se puede configurar un Nombre de Dominio Completamente Calificado (FQDN) en un servidor de nombrado DNS con ambas direcciones IPv4 e IPv6 y eventualmente este puede ser consultado para proveer información acerca de la disponibilidad de un nodo sobre IPv4 o IPv6. Una aplicación que soporta ambos stack's IPv4 e IPv6 solicitará al servicio de nombrado le resuelva FQDN en ambos tipos de direcciones, pero generalmente dará preferencia a las direcciones IPv6. La arquitectura de la capa IP dual y su forma de comunicación se observa en la Figura 7. *[12]*

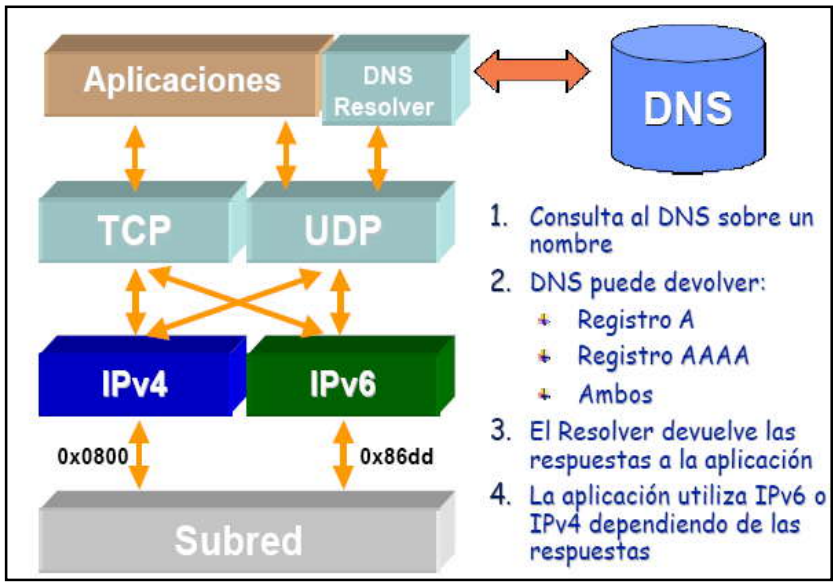


Figura 7: Esquema del mecanismo Dual Stack www.internetng.dit.upm.es

2.2 Túneles[15]

Los túneles encapsulan un paquete IPv6 dentro de un paquete IPv4 para atravesar redes que aun no han sido migradas. El paquete es

[15] RFC 2893 - Mecanismos de transición para hosts y router IPv6. Agosto 2000

desencapsulado al llegar al destino, que deberá ser un nodo IPv6 o dual stack. *[13]*

Los túneles pueden ser configurados de diferentes formas para el tráfico del túnel IPv6 entre nodos IPv6/IPv4 sobre una infraestructura IPv4, las cuales se describen en la Figura 8:

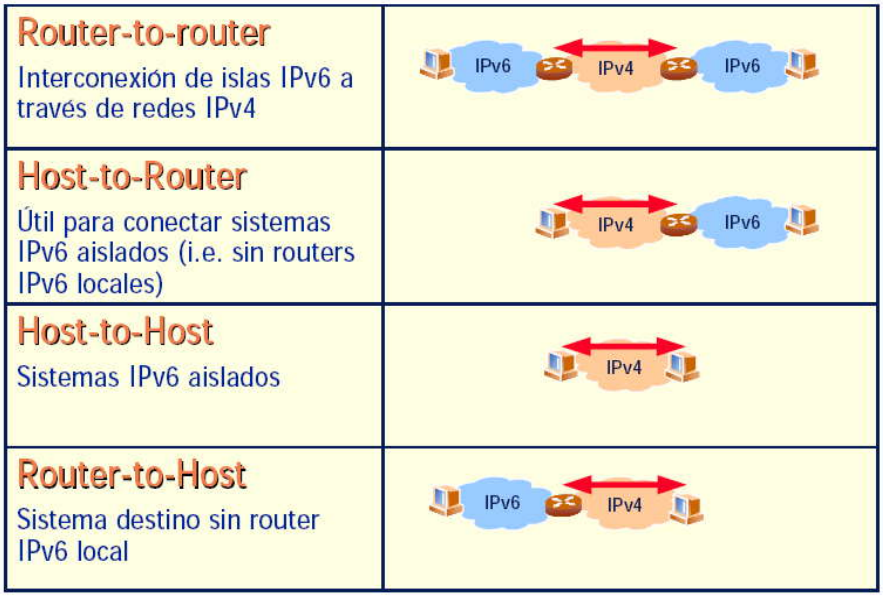


Figura 8: Tipos de configuración de túneles www.internetng.dit.upm.es

Entre los mecanismos de transición de los protocolos IPv4 a IPv6 mediante túneles se encuentran los siguientes:

2.2.1 Manuales/Automáticos

Los túneles manuales configuran manualmente el mapeo de direcciones de IPv6 a IPv4 en los puntos finales del túnel. El túnel automático utiliza direcciones IPv6 compatibles con IPv4. Los extremos finales del túnel se determinan por el uso de las interfaces lógicas del túnel, las rutas y las direcciones IPv6 de origen y destino.

2.2.2 6to4[16]

Se configura automáticamente, en este mecanismo los extremos del túnel están determinados por las direcciones globales IPv4 encapsuladas dentro de direcciones IPv6 *6to4*.

Cuando se utilizan hosts 6to4, una infraestructura de enrutamiento IPv6 en sitios 6to4, un enrutador 6to4 en los límites del sitio y un enrutador de retransmisión 6to4, son posibles los tipos de comunicación siguientes:

1. **Un host 6to4 se puede comunicar con otro host 6to4 en el mismo sitio**:

   Este tipo de comunicación está disponible mediante la infraestructura de enrutamiento IPv6, que proporciona accesibilidad a todos los hosts del sitio.

2. **Un host 6to4 se puede comunicar con hosts 6to4 de otros sitios de la red Internet IPv4**:

   Este tipo de comunicación se produce cuando un host 6to4 reenvía al enrutador 6to4 del sitio local el tráfico IPv6 que está destinado a un host 6to4 de otro sitio. El enrutador 6to4 del sitio local encapsula el tráfico IPv6 con un encabezado IPv4 y lo envía al enrutador 6to4 del sitio de destino en Internet. El enrutador 6to4 del sitio de destino quita el encabezado IPv4 y reenvía el paquete IPv6 al host 6to4 correcto, para lo que utiliza la infraestructura de enrutamiento IPv6 del sitio de destino.

3. **Un host 6to4 se puede comunicar con hosts de Internet IPv6:**

   Este tipo de comunicación se produce cuando un host 6to4 reenvía al enrutador 6to4 del sitio local el tráfico IPv6 que está destinado a un host de Internet IPv6. El enrutador 6to4 del sitio local encapsula el tráfico IPv6 con un encabezado

[16] RFC 3056 - Conexión de Dominios IPv6 a través de nubes IPv4. Febrero 2001

IPv4 y lo envía a un enrutador de retransmisión 6to4 que está conectado a la red Internet IPv4 y la red Internet IPv6. El enrutador de retransmisión 6to4 quita el encabezado IPv4 y reenvía el paquete IPv6 al host de Internet IPv6 apropiado mediante la infraestructura de enrutamiento IPv6 de la red Internet IPv6.

La Figura 9 ilustra el mecanismo 6to4 representado en redes 6to4 individuales. Cada sitio tiene un router configurado con una conexión de red IPv4 y con la capacidad de crear automáticamente un túnel 6to4 a través de la red IPv4 para que los sitios de red se puedan interconectar. *[14]*

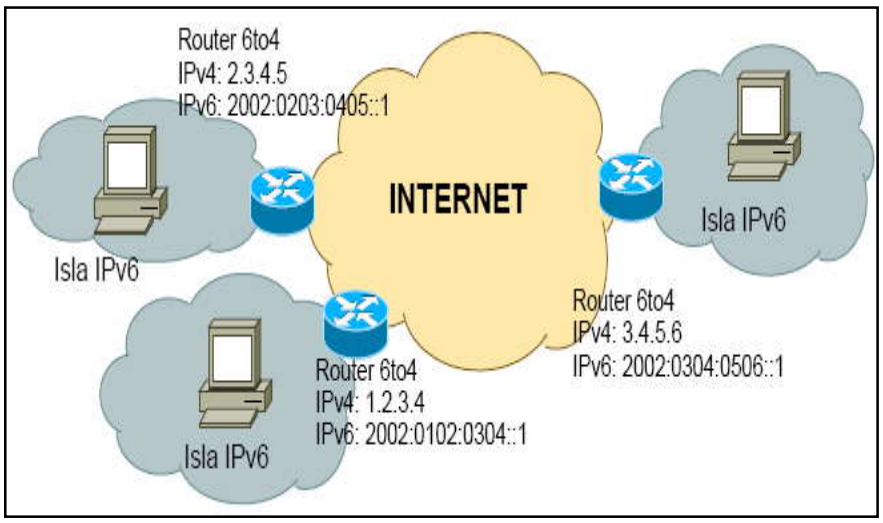


Figura 9: Esquema del túnel 6to4 www.um.edu.ar

2.2.3 Brokers[17]

Este mecanismo actúa como servidor sobre la red IPv4, recibe peticiones de nodos con dual stack para configurar túneles automáticamente, estas peticiones son enviadas vía http sobre IPv4 por el nodo que se quiere configurar el túnel. La arquitectura del túnel Broker se muestra a continuación en la Figura 10. *[15]*

[17] RFC 3053 - Ipv6 Tunnel Broker. Enero 2001

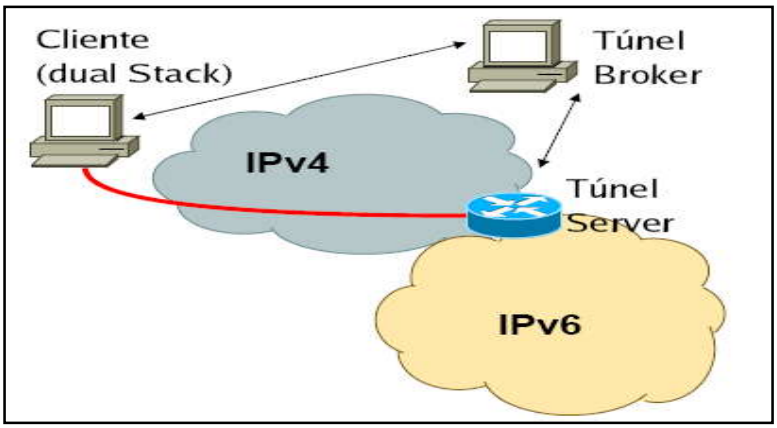


Figura 10: Esquema del túnel Broker www.codarec.frm.utn.edu.ar

2.2.4 6over4[18]

Este mecanismo es también conocido como túnel de multidifusión de IPv4, El túnel 6over4 permite la comunicación entre nodos IPv6 e IPv4 mediante IPv6 a través de una infraestructura IPv4. En 6over4 se utiliza la infraestructura IPv4 como vínculo con capacidad de multidifusión. Para que 6over4 funcione correctamente, la infraestructura IPv4 debe estar habilitada para multidifusión IPv4. Este tipo de mecanismo de transición se muestra en la Figura 11.

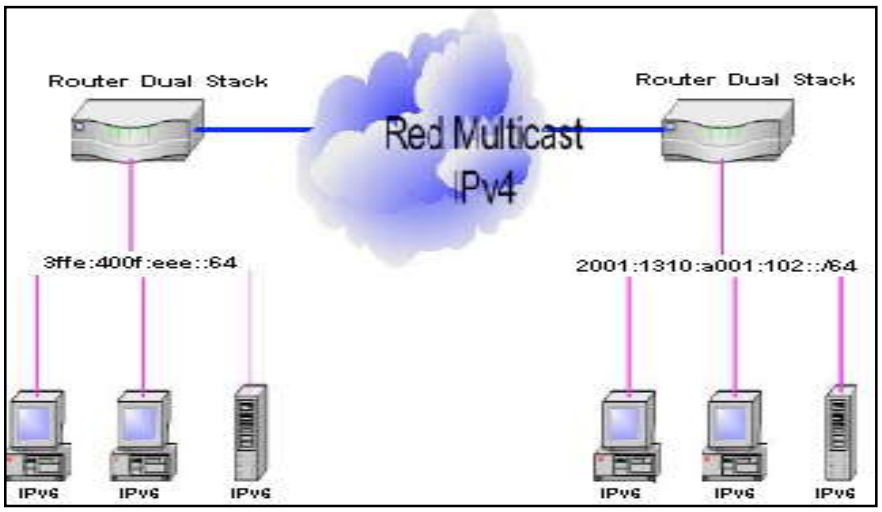


Figura 11: Esquema del túnel 6over4 www.consulintel.es

[18] RFC 2529 - Transmisión de paquetes IPv6 sobre IPv4. Marzo 1999

2.2.5 Teredo[19]

Este tipo de túnel fue diseñado para garantizar conectividad IPv6 a nodos con dual stack que están localizados detrás de dispositivos NAT sobre dominios IPv4. Teredo define una manera de encapsular paquetes IPv6 en datagramas UDP IPv4 que pueden ser dirigidos a través de dispositivos NAT y en internet IPv4. La Figura 12 muestra el esquema en el que un cliente se comunica a través de un túnel Teredo con hosts IPv6 nativos.*[16]*

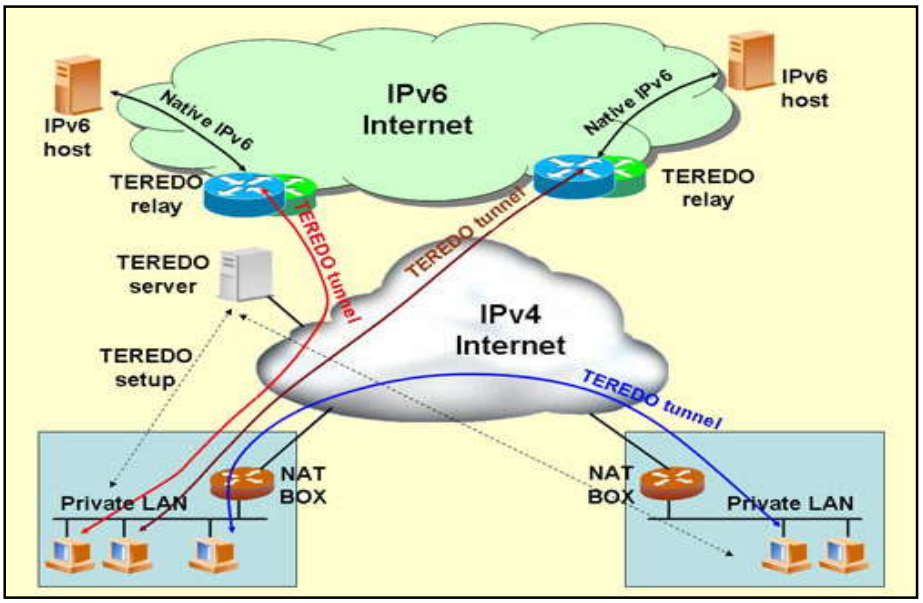


Figura 12: Esquema del túnel Teredo www.spain.ipv6tf.org

2.2.6 ISATAP[20]

El túnel Isatap (Intra Site Automatic Tunnel Addresing Protocol), permite crear túneles IPv6-in-IPv4 automáticamente dentro de un sitio IPv4. Cada *host* solicita a un enrutador dentro del sitio IPv4 una dirección IPv6 e información de enrutamiento, de esta manera, los paquetes enviados al Internet IPv6 son enrutados a

[19] RFC 4380 - Teredo: Tunneling IPv6 sobre UDP. Febrero 2006
[20] RFC 4214 - Intra Site automático túnel abordar Protocol (ISATAP). Octubre 2005

través del enrutador ISATAP y los paquetes destinados hacia otros hosts dentro del mismo sitio son entregados directamente mediante túneles ISATAP. *[17]*

Las direcciones IPv6 se configuran automáticamente mediante el protocolo "descubrimiento de enrutador" ISATAP, aunque también pueden ser configuradas de manera manual. La Figura 13 que se presenta a continuación, muestra el esquema de funcionamiento de los túneles Isatap.

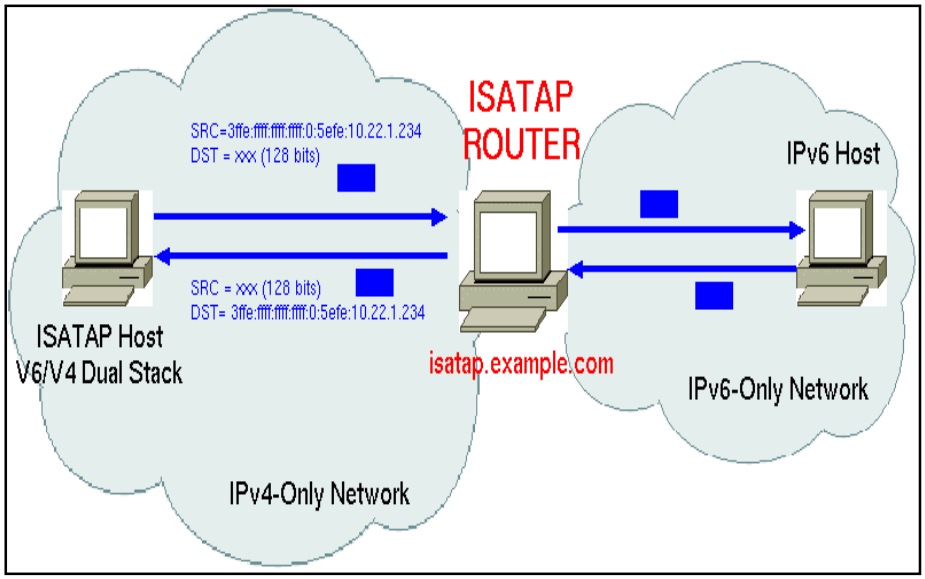


Figura 13: Esquema del túnel ISATAP www.isatap.example.com

2.3 Traducción

Este mecanismo de transición permite a un nodo que solo cuenta con el stack IPv6 comunicarse con otro nodo que solo tiene el stack IPv4. Sin embargo, ésta técnica requiere tener habilitados mecanismos de traducción entre IPv4 e IPv6 en los enrutadores de ambas redes. La principal desventaja es que todo el peso de este mecanismo de transición recae en los dispositivos encargados de hacer dicha traducción, a los que no siempre se tiene acceso. *[18]*

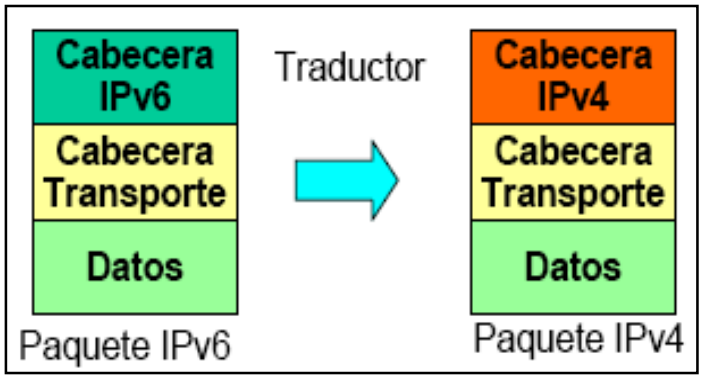


Figura 14: Esquema del mecanismo de traducción www.ipv6.codarec.frm.utn.edu.ar

2.3.1 NAT-PT[21]

El mecanismo de traducción NAT-PT se encarga de definir direcciones y protocolos. Se utiliza para comunicaciones entre hosts que son sólo IPv6 e IPv4 respectivamente, NAT (usa el mecanismo NAT para la asignación de la dirección IPv4) + el Protocolo de Traducción (usa el mecanismo SIIT), este mecanismo realiza la traducción IPv4/IPv6 y se mantiene el estado mientras dura la sesión. El flujo de información en NAT-PT se muestra a continuación en la Figura 15. *[19]*

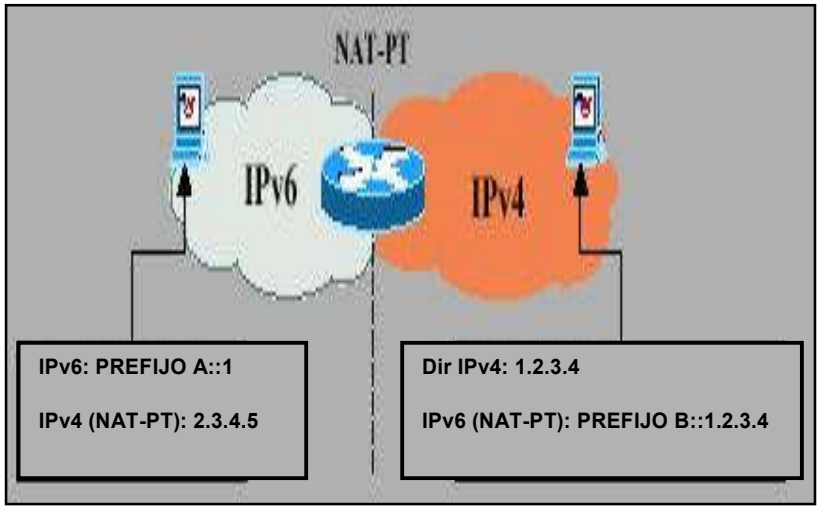


Figura 15: Esquema de traducción NAT-PT www.cu.ipv6tf.org

[21] RFC 2766 – NAT-PT. Febrero 2000

El IETF ha desarrollado algunos mecanismos de transición y coexistencia entre los protocolos IPv4 e IPv6, estos mecanismos implican la utilización de herramientas de ingeniería necesarias para definir estrategias de evolución. Elegir los mecanismos más convenientes, decidir dónde y cómo desplegarlos no es sencillo, por lo cual están siendo evaluados exhaustivamente por los fabricantes de routers y ordenadores.

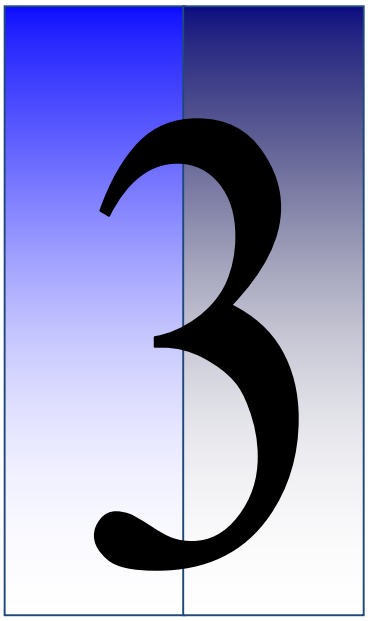
El despliegue del protocolo IPv6 se está realizando tanto en redes académicas como en redes comerciales en todo el mundo, es así que los fabricantes de equipos como DEC, Apple, Hewlett Packard, Novell, Microsoft, Compaq, 3Com, Cisco, Sun Microsystems, Nokia, Extreme Networks, entre muchos otros, están empezando a entregar computadoras, servidores, enrutadores y otros dispositivos con IPv6. Muchas organizaciones están trabajando en manejadores de dispositivos (drivers) para el sistema operativo UNIX BSD, Linux, y otros. El servidor Windows 2003 de Microsoft contempla aplicaciones y componentes bajo IPv6; un navegador de Internet, un cliente FTP y un cliente Telnet. Fabricantes de software de red (Trumpet, Interpeak, Mentat, etc.) han desarrollado una gran variedad de soporte para IPv6 en aplicaciones de red y software de comunicaciones (FTP, navegador Mozilla, Apache Web server, Sendmail). *[20]*

El mecanismo de transición más utilizado es Dual Stack (doble pila) IPv6/IPv4. Requiere que los hosts y los routers soporten ambas versiones de IP y, por tanto servicios y aplicaciones tanto IPv4 como IPv6, se han realizado varios experimentos que han comprobado la coexistencia de ambos protocolos.

Otros mecanismos de transición son los basados en traductores o en túneles, los cuales permitirán la interoperabilidad de los nuevos sistemas que sólo tengan IPv6 con la versión 4 del protocolo IP. Uno de los mecanismos, denominado NAT-PT, está basado en NAT permite acceder a servicios IPv4 desde una red privada IPv6.

Probablemente un problema de mayor envergadura sea la migración de aplicaciones a IPv6 los fabricantes de equipos podrán proveer funcionabilidad libre, en forma de una actualización, asegurando que las versiones posteriores del software de administración de red soportarán el nuevo esquema. Las aplicaciones IPv6 también utilizan TCP, UDP y el interfaz de sockets. El interfaz de sockets ha sido adaptado en sus múltiples versiones para utilizar IPv4, IPv6 o doble pila. Su uso es muy similar al que se hacía en IPv4, pero incluye pequeñas diferencias que obligan a realizar nuevas versiones de las aplicaciones existentes, para poder migrar a IPv6.

La migración de aplicaciones de IPv4 a IPv6 no es difícil si éstas se han diseñado haciendo un uso adecuado de esta interfaz. Incluso, algunos lenguajes hacen que la migración sea prácticamente transparente. La migración de todas las aplicaciones existentes necesitará un enorme volumen de trabajo, la mayor dificultad está en la cantidad de aplicaciones que hicieron mal uso de las direcciones IPv4 y del interfaz de sockets, que requieren un rediseño significativo de la aplicación.



Capítulo 3

DISEÑO DE LA PROPUESTA

3. INFRAESTRUCTURA ACTUAL DE LA RED DE LA EXTENSIÓN UNIVERSITARIA DE ZAMORA

La UTPL Extensión Zamora cuenta con una red LAN que es la que brinda servicio a los usuarios del campus universitario. La actual infraestructura de la Red Académica de nuestra Universidad es soportada bajo el protocolo IPv4, es por ello que es posible que se experimenten desempeños no deseables que repercutan directamente sobre los servicios que se desean ofrecer.

Los equipos que componen la estructura de la red en la extensión universitaria de Zamora se detallan a continuación.

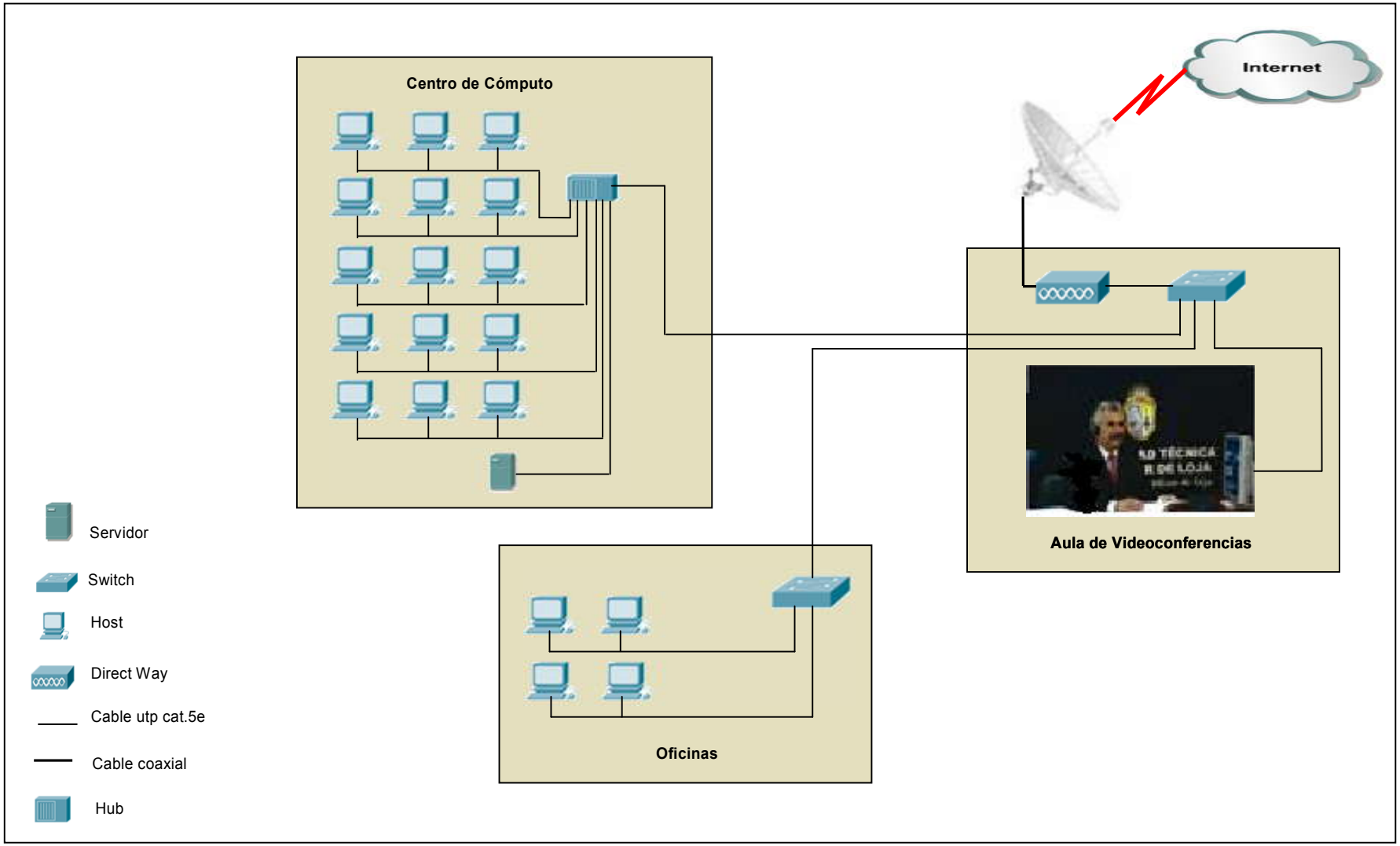
- En el área de Videoconferencias se encuentra un modem Direct Way el cual se encarga de decodificar la señal satelital, además de un switch 3Com de 24 puertos y una computadora IBM, es en este departamento desde donde se provee de Internet a las demás áreas de trabajo de la Extensión Universitaria.

- En el Laboratorio de Computación existen 16 computadoras de las cuales una funciona como servidor proxy a si mismo existe un Hub 3Com de 24 puertos, al cual se enlazan los 16 equipos.

En el departamento que corresponde a la dirección, secretaria, contabilidad, sala de catedráticos y biblioteca existe un switch 3Com de 16 puertos, las computadoras conectadas a este equipo suman en un total de 4.

Para tener una idea de la topología de red de la Extensión Universitaria de Zamora, a continuación se presenta un esquema, en el cual se puede evidenciar que los equipos que conforman la red se encuentran desactualizados en los requerimientos necesarios para poder permitir un mejor desempeño en la conectividad para el envío y recepción de datos.

ESQUEMA DE RED DE LA EXTENSIÓN UNIVERSITARIA DE ZAMORA



Análisis de Hardware, Software y Aplicaciones

A continuación se encuentra detallado el hardware y software con el que cuenta la extensión universitaria de Zamora, es por ello que se ha elaborado la Tabla 6 en la que se presenta las descripciones de los equipos de la Extensión Universitaria.

Descripción	Marca	Departamento	Procesador	RAM	HD	Plataforma	Aplicación
PC1 – PC 16	IBM	Cómputo	Pentium IV 1,8 GHz.	256MB	40GB	Windows XP SP2	F-Secure Client
PC18	IBM	Video Conferencias	Pentium IV 1,8 GHz.	256MB	40GB	Windows XP SP2	One Touch F-Secure Client
PC19	IBM	Dirección	Pentium IV 1,8 GHz.	256MB	40GB	Windows XP SP2	F-Secure Client
PC20	IBM	Sala de Profesores	Pentium IV 1,8 GHz.	256MB	40GB	Windows XP SP2	F-Secure Client
PC21	IBM	Contabilidad	Pentium IV 1,8 GHz.	256MB	40GB	Windows XP SP2	F-Secure Client
PC22	IBM	Secretaria	Pentium IV 1,8 GHz.	256MB	40GB	Windows XP SP2	F-Secure Client Acceso al Sistema Académico

Tabla 6: Detalle de los equipos existentes en la UTPL Extensión Zamora

3.1 Selección del mejor Mecanismo para la Transición de la LAN

La presente fase tiene por objetivo definir el mecanismo de transición y la configuración de equipos de direccionamiento. La elección del mecanismo se realiza tomando en cuenta el esquema de red de la Extensión Universitaria de Zamora así como los equipos de la misma.

Descripción de los Mecanismos de Transición:

En la Tabla 7 se hace referencia a los principales mecanismos de transición de entre los cuales se citaran ventajas y desventajas para de esta manera realizar la selección del mecanismo de transición a implementar.

Mecanismo	Conectividad	Descripción	Ventajas	Desventajas
Dual Stack	Solo entre sistemas del mismo tipo (IPv4-IPv4, IPv6-IPv6)	• Trabaja con ambos protocolos (IPv4/IPv6). • Procesa sólo los encabezados IP. • Uno de los más populares dentro de su tipo. • Se basa en DHCP y direcciones compatibles para asignación de direcciones.	Es fácil de implementar. Es la solución inmediata más accesible. Permite a los nuevos dispositivos IPv6 relacionarse rápidamente con los demás dispositivos	No trabaja en ambientes mixtos (IPv4 sobre IPv6 y viceversa). Si la red no es IPv6, no se beneficia de las características de esta versión
6over4	IPv6 a IPv6 sobre IPv4	• Se comporta como una red virtual	Permite la autoconfiguración. Conserva todas las características de IPv6	Necesita soporte de ruteo multicast (IPv4 raramente cuenta con este soporte)
6to4	IPv6 a IPv6 sobre IPv4	• Crea túneles automáticamente. • Algoritmo más popular dentro de su clase.	Ayuda a conectar redes IPv6 aisladas entre sí.	No funciona en redes con equipos de bajas características.
NAT-PT	De IPv6 a IPv4 y de IPv4 a IPv6	• Traductor estático que utiliza el algoritmo SIIT.	Actúa como un servidor Proxy. Utiliza direcciones temporales	Las mismas desventajas que con NAT (problemas en conexiones abiertas).

Tabla 7: Descripción de los mecanismos de Transición existentes

Dentro de los mecanismos estudiados en el capítulo 2, se ha seleccionado inicialmente Dual Stack o doble pila considerando que mediante esta técnica permitirá reducir el impacto (costo, tiempo y funcionalidad de las aplicaciones) ya que éste mecanismo no requiere duplicar redes ni interfaces de red para que los sistemas accedan a IPv4 o a IPv6. Sólo es necesario que los sistemas operativos de los ordenadores y routers sean capaces de utilizar ambas pilas de protocolos en paralelo, distinguiendo el paquete en el momento de la

recepción por medio de la cabecera de nivel de red y más concretamente a través del campo de versión de protocolo IP.

Dual Stack, es un mecanismo de transición básico diseñado para que los clientes IPv6 sean compatibles con los clientes IPv4, de manera que al configurar los equipos (switches, routers y hosts), éstos permitirán enviar y recibir paquetes IPv6 e IPv4 sin necesidad de realizar traducción de paquetes.

Ventajas de Dual Stack:

- Pueden coexistir en una misma organización.
- Evita problemas con los mecanismos de traducción.
- Las aplicaciones (o librerías) escogen la versión de IP a utilizar.
- Selección de la versión está basada en la resolución de nombres y la preferencia de la aplicación.

Para realizar la transición es necesario crear en primer instancia una red de pruebas en la cual se implementará Dual Stack; dado el esquema de red de la UTPL el cual analizaremos en lo posterior primero hay que realizar las respectivas configuraciones para que los equipos soporten doble direccionamiento (Dual Stack ó Doble Pila) y de esta manera lograr que la extensión universitaria de Zamora se convierta en una isla IPv6 pero para que sea posible la comunicación entre la isla IPv6 (Zamora) con nodos "Dual Stack" utilizaremos el mecanismo de transición túneles. Como en Internet se ejecuta comúnmente IPv4, los paquetes de IPv6 de la isla deben desplazarse por Internet a través de túneles hacia las redes IPv6 de destino. En donde los routers IPv6/IPv4 interconectados con una infraestructura IPv4 pueden transportar paquetes (voz, datos y video) entre las dos versiones del protocolo IP. [ver Figura 9].

Luego de que la red cuente con doble direccionamiento (Dual Stack ó Doble Pila), seguidamente se procederá a configurar los equipos para contar con el mecanismo de Transición seleccionado, el cual es "***Túnel 6to4***".

3.2 Activación de ipv6 en los equipos remotos

Para la realización del presente proyecto de tesis se ha implementado una red de pruebas, en la cual se realizará todas y cada una de las respectivas configuraciones necesarias para contar con Dual Satck (doble pila), luego se debe configurar los equipos a usarse (routers, switchs y pc´s), para finalmente realizar la transición completa del esquema de red en la Extensión Universitaria de Zamora. El hardware y software utilizados para la red de pruebas se detallan en la Tabla 8.

CARACTERÍSTICAS	PC1	PC2
Procesador	Pentium IV 1,8 GHz.	Pentium IV 1,8 GHz.
Memoria RAM	256 MB.	256 MB.
Disco Duro	40 GB.	40 GB.
Tarjeta de red	FastEthernet 100 Mbps.	FastEthernet 100 Mbps.
Plataforma	Linux Centos 4.7	Windows XP SP2
Soporte IPv4 e IPv6	SI	SI
Características del Switch		
Modelo	3COM Baseline 2016	
Número de puertos	16 (100 Mbps.)	
Soporte IPv4 e IPv6	Para pruebas no necesario (implementación SI)	

Tabla 8: Características de los equipos de la red de pruebas

Para el presente proyecto de Tesis, se realizó un esquema de laboratorio de pruebas, el cual se presenta en la Figura 16, el mismo que establece el enlace de comunicación entre los equipos del Host 1 con Sistema Operativo Windows y el Host 2 con Sistema Operativo Linux, ésta comunicación se la estableció con un switch 3Com de 24 puertos, dicho laboratorio se lo realizó con la finalidad de configurar las Direcciones en DualStack (Doble pila – IPv4 e IPv6).

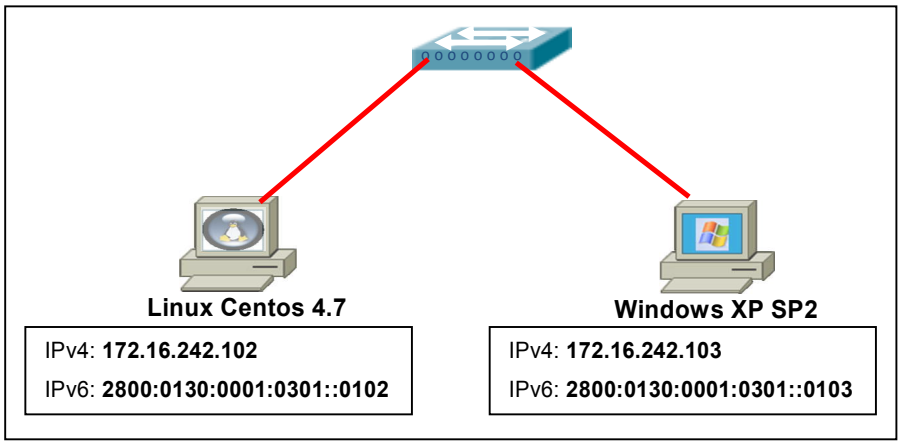


Figura 16: Esquema de la red de pruebas

Requisitos de prueba para el soporte de Dual Stack:

- Hardware y Software con soporte IPv6.
- Configuración de los dispositivos a nivel de S.O. para utilizar direcciones IPv6.
- Configuración en diferentes S.O. para gestionar las preferencias entre v4 y v6 en caso de que el host destino tenga ambas direcciones.
- Configuración de las aplicaciones de red para que soporten ambos tipos de direccionamiento.

La configuración detallada de IPv6 tanto en Windows como en Linux se encuentra en el Anexo [1].

3.3 Implementación del túnel 6to4

Una vez que hemos realizado la implementación de Dual Stack, es necesario crear un enlace mediante un túnel para el transporte de paquetes IPv6 ya que debido a que el encaminador del ISP (Proveedor de Servicio de Internet) no soporta Dual Stack, será necesario crear un túnel con el cual Zamora se conectara con Loja; en el capitulo anterior estudiamos la clasificación de túneles entre los más utilizados se encuentran:

- 6to4
- 6over4
- Teredo
- Isatap

De entre los cuales se ha elegido como el más conveniente a 6to4 ya que se adapta a la estructura de red de la UTPL.

Este mecanismo se puede aplicar para comunicar redes IPv6 aisladas por medio de la red IPv4. El router extremo de la red IPv6 crea un túnel sobre IPv4 para alcanzar la otra red IPv6. Los extremos del túnel son identificados por el prefijo del sitio IPv6. Este prefijo consiste en 16 bits fijos que indican que estamos utilizando la técnica 6to4 más 32 bits que identifican al router externo del “sitio”.

Un efecto secundario de 6to4 es que deriva automáticamente un prefijo /48 de una dirección IPv4. De esta forma, los 'sitios' pueden empezar a utilizar IPv6 sin solicitar nuevo espacio de direccionamiento.

El nodo de entrada del túnel (nodo de encapsulamiento) crea un paquete IPv4 en el que encapsula el paquete IPv6, y lo transmite encapsulado. El header IPv4 contiene las direcciones fuente y destino y el cuerpo del paquete contiene el header IPv6 seguido inmediatamente por los datos.

El nodo de salida del túnel (nodo de desencapsulamiento) recibe el paquete encapsulado, elimina el header IPv4, actualiza el header IPv6 y procesa el paquete IPv6 recibido.

Las técnicas de túnel se clasifican según el mecanismo por el cual el nodo de encapsulamiento determina la dirección del nodo al final del túnel. En este caso se ha seleccionado a Router to Router.

***Router-to-Router*:** Los routers IPv6/IPv4 interconectados con una infraestructura IPv4 pueden pasarse entre sí paquetes IPv6. En este caso el túnel abarca un segmento del trayecto que toma el paquete IPv6.

ESQUEMA DE RED PROPUESTO PARA LA TRANSICIÓN

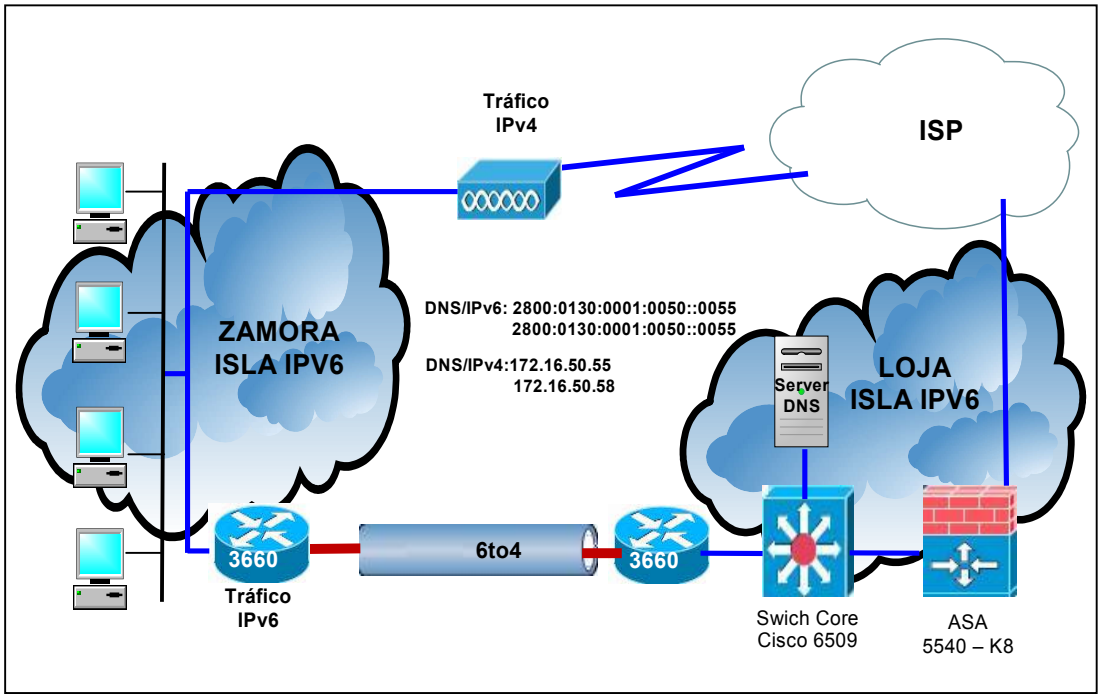


Figura 17: Esquema de red propuesto para la transición

Una vez que tenemos la información necesaria para construir el túnel empezamos por describir las configuraciones de los routers para el enlace 6to4.

La Figura 17 muestra la topología de red propuesta para la transición de IPv4 a IPv6 en la cual se especifican sus principales componentes los mismos que estarán involucrados en el diseño de la propuesta del presente proyecto de investigación.

En la isla IPv6 Zamora se utilizará el router Cisco 3660 con IOS 12.3 (14) T4, dicho sistema operativo tiene la facilidad de manejar IPv6 tanto su direccionamiento como para la creación de túneles necesarios para hacer la conexión entre equipos, en el router se configurará doble direccionamiento (Dual Stack) por donde se transportarán paquetes (voz, datos, video) mediante el túnel propuesto “6to4” hacia la isla IPv6 Loja.

Para la configuración de IPv4, cada equipo se configura manualmente con la dirección IP, máscara de subred, puerta de enlace predeterminada o "Gateway" y dirección IP del servidor DNS adecuadas. En el caso de IPv6 la configuración se realiza utilizando servidores de Protocolo de configuración dinámica de host (DHCP, *Dynamic Host Configuration Protocol*), así mismo las direcciones IP se las obtendrá del servidor DNS.

Para poder transportar el tráfico IPv6 utilizaremos el mecanismo de transición túneles 6to4. A través de éste se enviarán los paquetes IPv6 encapsulados en paquetes IPv4 hacia la red de la Universidad Matriz en la ciudad de Loja y de esta manera lograr que la red de la extensión Zamora pueda tener comunicación con nodos IPv6/IPv4. Cuando se requiera de recepción o envío de paquetes IPv4 se hará uso de un encaminador que se enlazará directamente con el ISP. Para la creación de los túneles se necesitan de algunos requisitos:

- Dirección IPv4 de Router Zamora: 192.168.5.1
- Dirección IPv4 del Router Loja: 192.168.1.2
- Dirección IPv6 para el túnel:

  - 2800:0130:0001:0010::0085/64 para el equipo remoto (Loja).
  - 2800:0130:0001:0301::0126/64 para el equipo local (Zamora).

El principio básico de 6to4 es utilizar la infraestructura IPv4 existente para entregar paquetes IPv6 y por lo tanto hará uso del enrutamiento en IPv4. Lo primero que debemos hacer es verificar la conexión IPv4 entre ambas islas. En los routers Zamora y Loja vamos a utilizar direcciones IPv4 para los seriales así como para las LAN internas y el protocolo de enrutamiento que se usará para el laboratorio será RIP. A continuación se detalla su configuración:

ROUTER ZAMORA

```
Router> enable
Router# configure terminal                    *// Nombre del Router
Router(config)#hostname Zamora
zamora(config)# enable secret (password)      *// password encriptado
Zamora(config)# line console 0                *// password de consola
Zamora(config-line)#password (password)
Zamora(config-line)# login
Zamora(config-line)# line vty 0 4             *// Se crean 4 sesiones de Telnet para atención
Zamora(config-line)# password (password)          remota
Zamora(config-line)# login
Zamora(config-line)# exit

Configuración de la Interfaz Serial 0 para la LAN interna de la isla Zamora

Zamora(config)#interface serial 0/0
Zamora(config-if)#  description Conexión con el router de Loja
Zamora(config-if)# ip address 192.168.5.1     255.255.255.0
Zamora(config-if)# clock rate 56000
Zamora(config-if)# no shutdown
Zamora(config-if)#exit

Configuración de la Interfaz Fastethernet 0

Zamora(config)# interface fastethernet 0/0
Zamora(config-if)#description interface de la LAN interna de la Isla de Zamora
Zamora(config-if)#ip address 192.168.1.1    255.255.255.0
Zamora(config-if)#no shutdown
Zamora(config-if)#exit

Configuración del protocolo de enrutamiento

Zamora(config)#router rip
Zamora(config-router)#network 192.168.1.0
Zamora(config-router)#network 192.168.5.0
```

Figura 18: Configuración del Protocolo RIP, para las pruebas de Laboratorio en el router Zamora

ROUTER LOJA

```
Router> enable
Router# configure terminal                    *// Nombre del Router
Router(config)#hostname Loja
Loja (config)# enable secret (password)       *// password encriptado
Loja (config)# line console 0                 *// password de consola
Loja (config-line)#password (password)
Loja (config-line)# login
Loja (config-line)# line vty 0 4              *// Se crean 4 sesiones de Telnet para atención
Loja (config-line)# password (password)           remota
Loja (config-line)# login
Loja (config-line)# exit

Configuración de la Interfaz Serial 0 para la LAN interna de la isla Loja

Loja (config)# interface serial 0/0
Loja (config-if)#description Conexión con el router de Zamora
Loja (config-if)#ip address 192.168.1.2    255.255.255.0
Loja (config-if)#no shutdown
Loja (config-if)#exit

Configuración de la Interfaz Fastethernet 0

Loja(config)# interface fastethernet 0/0
Loja(config-if)#description interface de la LAN interna de la Isla de Loja
Loja (config-if)#ip address 192.168.4.1 255.255.255.0
Loja (config-if)#no shutdown
Loja (config-if)#exit

Configuración del protocolo de enrutamiento

Loja (config)#router rip
Loja (config-router)#network 192.168.1.0
Loja (config-router)#network 192.168.4.0
```

Figura 19: Configuración del Protocolo RIP, para las pruebas de Laboratorio en el router Loja

Una vez que se han configurado las interfaces y probado que existe conexión, entonces aquí tenemos nuestra infraestructura IPv4 lista entre las dos islas ahora se debe configurar el túnel.

- 6to4 es un mecanismo de router a router (específicamente los routers de borde de ambas islas) por lo tanto el router Zamora y Loja serán nuestros routers 6to4 en donde configuraremos el túnel.
- El principio básico que usa 6to4 es utilizar direcciones 6to4, esto es, direcciones que usan el prefijo 2002::/16; y dentro de este prefijo se incluirá (embeberá) la dirección IPv4 del router 6to4 en el cual se aplica el túnel, por lo tanto las direcciones 6to4 tienen el siguiente formato: 2002:direccion:ipv4:router6to4::/48

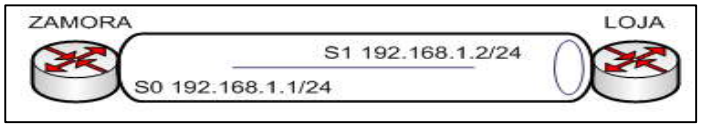


Figura 20: Seriales de los routers en IPv4 de Zamora y Loja, para las pruebas de Laboratorio

Para obtener las direcciones 6to4 se deberá primero transformar las direcciones IPv4 de los routers de Zamora y Loja a hexadecimales:

ZAMORA: 192.168.1.1 → **CO A8 01 01**, y luego la añadimos al prefijo asignado para las direcciones 6to4 con lo que la dirección 6to4 para el router de Zamora será la siguiente: 2002:**COA8:01 01::/**48

LOJA: 192.168.1.2 → **CO A8 01 02**, y luego la añadimos al prefijo asignado para las direcciones 6to4 con lo que la dirección 6to4 para el router de Loja sería la siguiente: 2002:**COA8:01 02::/**48

Ahora se configurará el router para que los hosts de la isla de Zamora se autoconfiguren con direcciones IPv6 de manera automática.

Configuración de la Fastethernet para la LAN interna de la isla Zamora, para que los hosts se autoconfiguren con direcciones IPv6:

- A continuación configuramos rutas estáticas que permiten dirigir el trafico ipv6 por el túnel configurado.

Zamora(config)#ipv6 route 2002::/16 tunnel 0

- A continuación configuramos el túnel en el router de Loja.

```
Zamora(config)# interface fa0/0
Zamora(config-if)#ipv6 address 2002:COA8:0101:1::/64
Zamora(config-if)#ipv6 enable
Zamora(config-if)#no shutdown
Zamora(config-if)#exit
Zamora(config)#ipv6 unicast-routing
Zamora(config)#exit

A continuación configuramos el túnel 6to4:

Zamora(config)# interface tunnel 0
Zamora(config-if)#description Tunel 6to4 hacia el router de Loja
Zamora(config-if)#no ip address
Zamora(config-if)#no ip redirects
Zamora(config-if)#ipv6 address 2002:COA8:0101::1/128
Zamora(config-if)#tunnel source Serial 0
Zamora(config-if)#mode ipv6ip 6to4
Zamora(config-if)#exit
```

Figura 21: Configuración de la Fastethernet para la LAN interna de la isla Zamora

Configuración de la Fastethernet para la LAN interna de la isla Loja, para que los hosts se autoconfiguren con direcciones IPv6.

A continuación configuramos rutas estáticas que permiten dirigir el trafico IPv6 por el túnel configurado.

Loja (config)#ipv6 route 2002::/16 tunnel 0

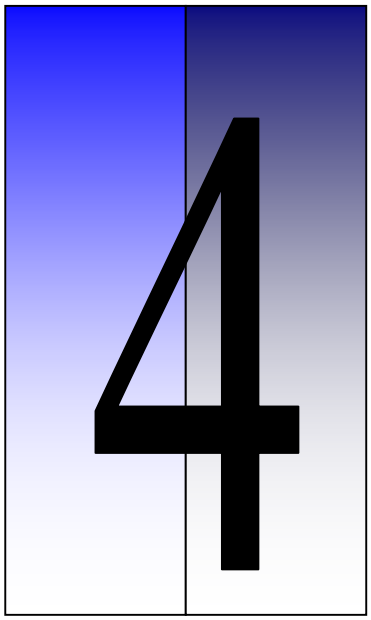
```
Loja(config)# interface fa0/0
Loja (config-if)#ipv6 address 2002:COA8:0102:1::/64
Loja (config-if)#ipv6 enable
Loja (config-if)#no shutdown
Loja (config-if)#exit
Loja (config)#ipv6 unicast-routing
Loja (config)#exit

•  A continuación configuramos el tunnel 6to4

Loja (config)# interface tunnel 0
Loja (config-if)#description Tunel 6to4 hacia el router de Zamora
Loja (config-if)#no ip address
Loja (config-if)#no ip redirects
Loja (config-if)#ipv6 address 2002:COA8:0102128
Loja (config-if)#tunnel source Serial 0
Loja (config-if)#mode ipv6ip 6to4
Loja (config-if)#exit
```

Figura 22: Configuración de la Fastethernet para la LAN interna de la isla Loja

Cuando el tráfico sea IPv4 se hará uso de un encaminador específico el mismo que se conectará directamente con el proveedor de Internet, esto sucederá únicamente cuando el tráfico sea solo direccionamiento IPv4.



ANÁLISIS Y DISCUSIÓN DE LA PROPUESTA

Capítulo

4. ESCENARIOS DE TRANSICIÓN A IPV6

La estructura de red con la que cuenta la extensión Universitaria de Zamora en la actualidad ha mantenido el buen funcionamiento y escalabilidad de la red en la versión 4 del protocolo IP, el presente proyecto de Tesis no busca reemplazar los servicios IPv4 existentes, la adopción exitosa de cualquier nueva tecnología, depende de la fácil integración con la infraestructura existente, objetivo propuesto por algunas entidades que quieren estar a la par con la tecnología, implementando mecanismos de transición maduros y estables para que fluyan los datos y demás aplicaciones tanto en IPv4 como en IPv6.

A continuación se presentan los diferentes escenarios de tráfico que existen dentro de la UTPL - Zamora para realizar la transición a IPv6; como ya lo analizamos no todos los equipos de red que intervienen soportan el mecanismo de transición Dual Stack, por lo cual se presenta como propuesta de solución final el mecanismo de transición Túnel "6to4" lo que permitirá la transición de dicha tecnología en la red de la UTPL, tomando en cuenta las recomendaciones realizadas en el capitulo 3 sobre los cambios que deben hacerse en los equipos de red correspondientes.

4.1 PRIMER ESCENARIO: Tráfico interno en el Campus de la UTPL – Zamora.

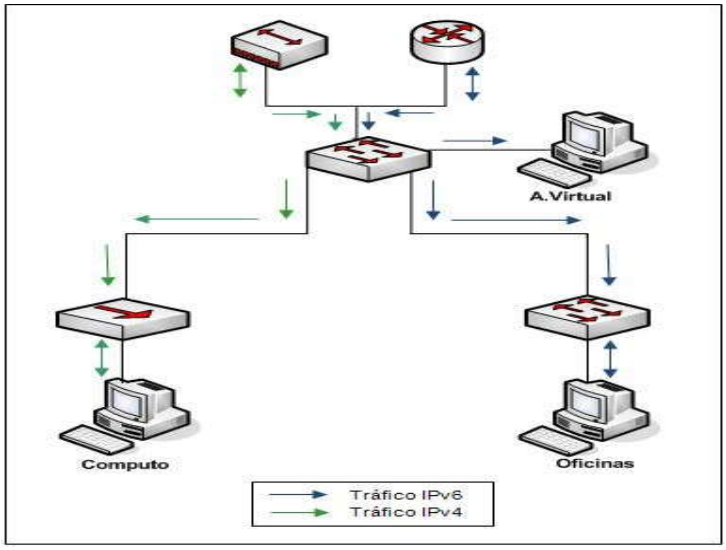


Figura 23: Flujo de tráfico interno en la UTPL - Zamora

El esquema que se propone como primera instancia involucra la activación de IPv6 en los servicios de Internet, los cuales fueron configurados en Doble-Pila para enviar y recibir paquetes en IPv4 - IPv6 o ambas en la infraestructura de red actual. Estos servicios entrarán en funcionamiento en Doble-Pila en el momento en el que los dispositivos de capa 2 y 3 soporten IPv6, de manera que en la extensión universitaria de Zamora fluirá tráfico en ambas versiones del protocolo IP. Ver figura 23.

4.2 SEGUNDO ESCENARIO: Tráfico en la conexión entre Zamora y Loja.

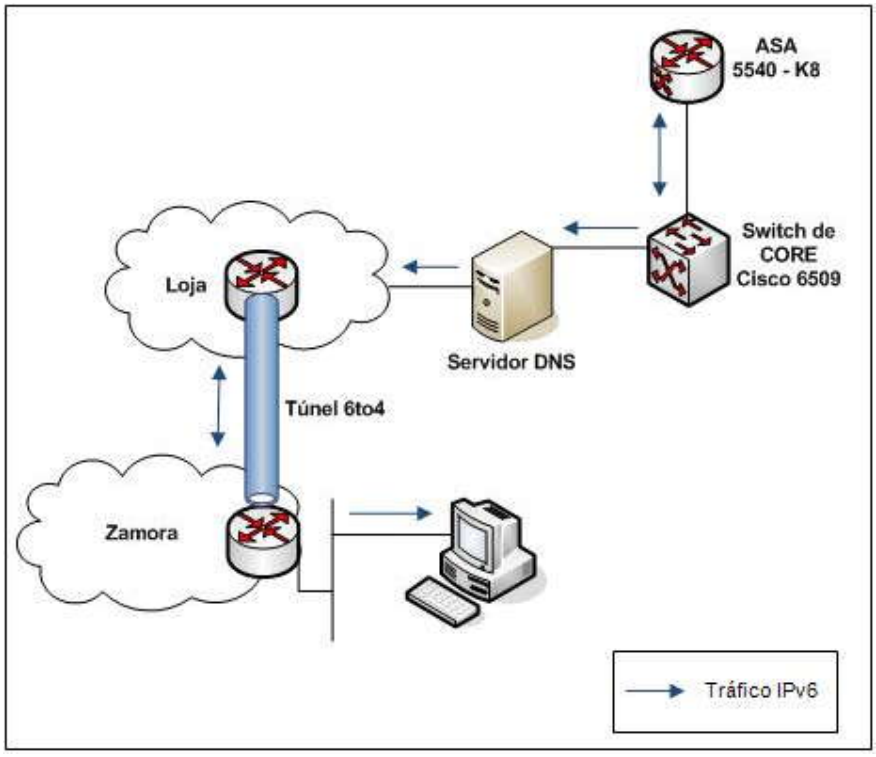


Figura 24: Flujo de tráfico Zamora – Loja

El escenario de prueba se describe a continuación:

VLAN	301
DIRECCIÓN IPv4	172.16.242.126
DIRECCIÓN IPv6	2800:0130:0001:0301::0126/64
MÁSCARA DE SUBRED	255.255.255.224
GATEWAY IPv4/IPv6	172.16.301.0 - 2800:0130:0001:0301::0000

DNS DE LA RED DE LA UTPL		
DNS	**IPv4**	**IPv6**
DNS Interno	172.16.50.58	2800:0130:0001:0050::0058
DNS Primario	200.0.31.155	2800:0130:0001:0222::0155
DNS Caching	172.16.50.55	2800:0130:0001:0050::0055

Tabla 9: Descripción de configuración del túnel

La Tabla 9 describe el esquema de red de la figura 24, en donde se define la forma en la que los equipos de la topología planteada obtienen una dirección IP, DNS y la puerta de enlace (Gateway).

Primeramente el cliente envía una petición al servidor DHCP para obtener una dirección, y de esta manera establecer la comunicación entre el cliente y el servidor, cuando el servidor recibe la petición, éste ofrece al cliente información de configuración IP (direcciones IP y dominios) mediante el DHCPOFFER y el cliente realiza un DHCPREQUEST, especificando los parámetros IP que necesita, de manera que el servidor que recibe el DHCPREQUEST formaliza la configuración enviando un DHCPACK, esto se realiza en la versión 4 del protocolo IP.

En cambio en el protocolo de la Nueva Generación tiene la característica de Autoconfiguración (Plug & Play - conectar y operar), por lo que los host que se conecten a la red Dual, que utilicen el tráfico IPv6 no tendrán la necesidad de realizar manualmente el direccionamiento IP, aunque también existe la posibilidad de realizar manualmente éste proceso de asignación de direcciones a los equipos de la red.[22]

En la figura 24 se observa como se realiza el flujo de tráfico para enlazar Zamora y Loja; el tráfico IPv6 hace uso del mecanismo de transición Túnel 6to4, este tipo de mecanismo permite que dominios IPv6 aislados se comuniquen con otros dominios IPv6 en primer instancia el nodo de entrada del túnel crea un paquete IPv4 en el que encapsula el paquete IPv6 y lo transmite encapsulado.

[22] Teleconferencia de Jordi Palet - Director de Lacnic España y miembro de IPv6 Task Force de Europa.

Las direcciones IPv4 de los extremos del túnel son determinados al extraerlos del prefijo global IPv6 de la dirección destino del paquete IPv6 a transmitir. Mientras que las direcciones IPv6 son autoconfiguradas.

4.3 TERCER ESCENARIO: Tráfico conexión a Internet.

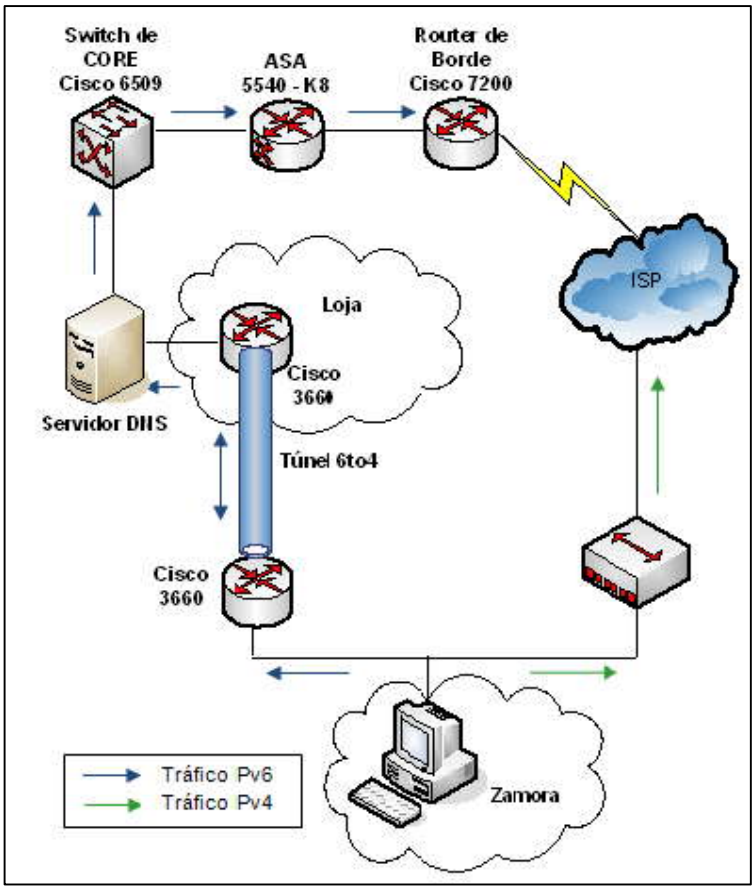


Figura 25: Flujo de tráfico IPv4 – IPv6 con conexión a Internet

Este proyecto de transición de direcciones IP se enfoca en mantener una plataforma dual sobre IPv4 e IPv6, por ello será necesaria la adopción de los mecanismos de coexistencia e interoperabilidad propuestos No se busca remplazar la red IPv4 sino mejorarla. Los equipos se plantean previo análisis de los recursos disponibles. Para lograr que en nuestra red universitaria fluya tráfico IPv6 como IPv4, se recomienda hacer uso de los equipos que se detallan en la Tabla 10:

Cantidad	Equipo	Marca	Modelo	Versión IOS
2	Router	Cisco	3660	12.3
1	Switch	Cisco	2950	12.1

Tabla 10: Equipos necesarios para el diseño de la propuesta del Túnel 6to4

Como se observa en la figura 25 para establecer la conexión a internet en la extensión universitaria de Zamora se inicia identificando el tráfico, para el efecto si el tráfico es IPv6 debe pasar a través del Túnel "6to4", llega al servidor DNS el cual tiene como función la traducción de nombres a direcciones IP y viceversa, con el propósito de comunicar la red LAN con la Internet, luego la transmisión pasa por el Switch de CORE y el Firewall ASA para finalmente llegar al router de borde y así enlazarse con el Proveedor de Internet.

Una vez establecida la conexión con otros dominios el tráfico que viene del exterior llega al router de borde, luego pasa por el Firewall ASA y finalmente por el Switch de CORE para transmitir el tráfico por el Túnel "6to4" hasta Zamora. Mientras que cuando el tráfico es IPv4 se conecta al Switch y luego con el proveedor de Internet como se muestra anteriormente en la figura 25.

4.4 Servicios IPv6 en la UTPL

La conectividad a IPv6 de los servidores en la red de la UTPL está empezando, muestra de ello es la migración de algunos servidores con los que cuenta actualmente la Universidad, es por ello que con la finalidad de tener una mejor funcionalidad Dual (IPv4 e IPv6) en el envío de datos de extremo a extremo y ante las funcionalidades que necesitan las redes actuales como QoS (Calidad de Servicio), Movilidad, Multicasting, etc., se considera que es necesario la migración del resto de servidores que existen en la Universidad.

Los servidores con los que cuenta la UTPL en IPv6 [Ver Tabla 11] se describen a continuación:

4.4.1 Servidor Monitoreo de la Red

Este servidor nos permite monitorear y controlar la red de la Universidad. Las aplicaciones instaladas en dicho servidor son:

- **Cacti:** Es una completa solución de graficado en red, diseñada para aprovechar el poder de almacenamiento, este paquete permite visualizar gráficamente el uso de servidores y equipos que tienen instalado y habilitado el protocolo snmp.

- **Nagios:** Es un sistema open source de monitorización de redes ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no es el deseado. Entre sus características principales figuran la monitorización de servicios de red.

4.4.2 Servidor de Correo Electrónico

Es una aplicación que permite enviar mensajes electrónicos de un usuario a otro en la red; a estos mensajes se los denomina correos. En este servidor se encuentran instaladas las siguientes aplicaciones:

- **Sendmail:** Es un agente de transporte de correo en Internet, cuya tarea consiste en "encaminar" los mensajes de forma que estos lleguen a su destino, además es utilizado para que el Nagios pueda enviar alertas hacia los correos electrónicos, esta aplicación soporta IPv6.

- **POP3:** El Post Office Protocol (POP3) se utiliza en clientes locales de correo para recibir correo, permite recuperar el correo y se almacenan localmente en el disco duro de las máquinas de los usuarios.

4.4.3 Servidor Proxy

Este servidor se encarga de bloquear el acceso a páginas y puertos determinados, registrando las conexiones realizadas mediante la autenticación del usuario. Además nos permite controlar el uso del

Ancho de Banda existente en la Universidad. En este servidor se encuentra instalada la siguiente aplicación:

- **Squid:** Es un programa de software libre que implementa un servidor proxy y un *demonio* para caché de páginas web, publicado bajo licencia GPL (Licencia Pública General). Además permite a varios computadores conectados a una red, obtener salida a Internet a través de un único computador, pudiendo así controlar el acceso a Internet.

4.4.4 Servidores DNS

La aplicación instalada en este servidor es el BIND 9.0 (Berkeley Internet Name Domain), que contiene el *named* para la resolución de los nombres y direcciones, viene con soporte nativo para IPv6, por lo que únicamente será necesario configurarlo.

- **DNS Interno:** Se encarga de resolver cada una de las peticiones DNS (resolución de direcciones a dominios y viceversa) internas; todas aquellas direcciones y dominios que se encuentran dentro de la subred 172.16.0.0

- **DNS Primario:** Se encarga de resolver las direcciones y dominios públicos; adicionalmente se comunica con el servidor secundario de Impsat y el DNS caching.

- **DNS Caching:** almacena los directorios accedidos y resueltos hacia el Internet, este servidor sirve backup al DNS Interno.

4.4.5 Servidor Hosting

Este servidor se encarga del funcionamiento del Servidor Web. Las aplicaciones instaladas se describen a continuación:

- **Apache:** Es un servidor web HTTP de código abierto para plataformas Unix (BSD, GNU/Linux, etc.), Windows, Macintosh y otras, que implementa el protocolo HTTP/1.1, ofrece soporte para host virtuales e IPv6.

- **Php (Hypertext Pre-processor):** Lenguaje de programación utilizado en la creación de contenido para sitios Web; viene con soporte nativo para IPv6.

- **Mysql:** Sistema de gestión de base de datos multiusuario, requerido para cumplir con las necesidades de los clientes en vista de que algunos de sus portales son desarrollados en esta herramienta.

No.	SERVIDOR	IPv4	IPv6	APLICACIONES
1	Monitoreo de la red	**172.16.50.57**	**2800:130:1:50::57**	Cacti Ver. 0.8.6h.fc3.rf Nagios Ver. 1.2-2.1.fc3.rf
2	Correo electrónico	**172.16.50.73**	**2800:130:1:50::73**	Sendmail Ver. 8.13.1-3 POP3
3	DHCP y Proxy	**172.16.50.54**	**2800:130:1:50::54**	Squid 2.0.6Stable6
4	DNS Interno	**172.16.50.58**	**2800:130:1:50::58**	BIND Ver. 9.2.1-16
	DNS Primario	**200.0.31.155**	**2800:130:1:222::155**	
	DNS Caching	**172.16.50.55**	**2800:130:1:50::55**	
5	Hosting	**172.16.80.14**	**2800:130:1:80::14**	Apache Ver. 2.0.52 PHP Ver. 4.3.9 MySQL Ver. 4.1.20-1

Tabla 11: Servicios en IPv6 de la UTPL con sus respectivas Aplicaciones

CONCLUSIONES:

- La realización del diseño de red propuesto en el presente proyecto de tesis se adapta básicamente a la topología actual que existe en la Extensión Universitaria de Zamora lo cual permite rápidamente entrar en el mundo IPv6. Esto hace que no sea necesario esperar a que los proveedores ISP (Internet Service Provider) nos den conectividad nativa a IPv6 para poder utilizar esta nueva tecnología.

- Las aplicaciones con soporte IPv6 que se encuentran funcionando en los diferentes servidores de la UTPL, han facilitado la configuración, implementación e integración del servicio evitando de esta manera inconvenientes futuros.

- Las características propias de IPv6 permiten que las aplicaciones instaladas en los servidores de la UTPL, provean de un servicio eficiente y de calidad a los múltiples usuarios con los que cuenta la Universidad.

- Según las características de la estructura de red de la Extensión Universitaria de Zamora, para poder realizar la transición a IPv6 es necesario que se realice en primera instancia la activación de Dual Stack en los equipos de la LAN, consiguiendo con esto una isla IPv6, finalmente para lograr la conectividad con el exterior se hará uso del mecanismo de transición “6to4” el cual permitirá la conectividad con los dos protocolos.

- Como se evidencia en el tercer escenario para que fluya tráfico en IPv6 se hará uso del túnel 6to4, mientras que cuando el tráfico sea IPv4 se conectará directamente con el ISP.

- Según las investigaciones realizadas se concluye que los equipos propuestos para la transición se adaptan eficientemente a la topología de la UTPL para lograr a futuro la implementación del presente proyecto de tesis.

- La implementación del presente proyecto de tesis en los centros asociados que posee la UTPL es el método más adecuado y de menor costo para lograr la migración parcial a IPv6.

- IPv6 mejora la transmisión eficientemente de una de las aplicaciones principales de la UTPL, la de videoconferencia, la misma que al contar con

éste nuevo protocolo permite una mayor y rápida transmisión para la impartición de clases o conferencias permitiendo asegurar la calidad de servicio de esa interacción.

- Para que exista la coexistencia de las dos versiones, se debe mantener la versión actual "IPv4", ya que la transición total de ésta nueva tecnología será progresiva. IPv6 no es una tecnología aislada, pues implica muchas interacciones con las tecnologías actuales y emergentes.

- El primer escenario muestra la solución presentada para lograr que en la Extensión Universitaria de Zamora fluya tráfico en ambas versiones del protocolo IP (IPv4 – IPv6), mediante los mecanismos Dual Stack y Túnel 6to4, permitiendo así la coexistencia de los mismos.

- Los escenarios planteados en el presente proyecto de Tesis para la transición a IPv6 en la Extensión Universitaria de Zamora, se implementaran una vez que se provean de los equipos necesarios planteados en los escenarios.

- El cambio de IPv4 a IPv6 no es una cuestión de migración, sino de integración y evolución que nos permitirá un crecimiento escalable y simple, en el diseño de red propuesto para la transición a IPv6 de la red Universitaria de Zamora.

- La migración de IPv4 a IPv6 es una tarea que se debe abordar de forma gradual. La primera medida ha de ser la instalación de routers que tengan capacidad para procesar los paquetes generados por ambos protocolos.

- La implementación de IPv6 en la red universitaria de la UTPL es un asunto de enorme trascendencia para el futuro de la Universidad. La UTPL ha experimentado la transformación de la era de las tecnologías de información en las diferentes áreas, siendo así que éstas han colaborado para no quedarnos rezagados en los avances de la tecnología, un ejemplo claro es que se está impulsando el desarrollo del protocolo de la nueva Generación, en lo referente a Seguridad, Multicast, Calidad de Servicio, Movilidad y Telefonía en IPv6.

RECOMENDACIONES:

- La topología de la red actual aunque cubre las expectativas de servicio para lo cual fue diseñada cabe mencionar que en el área de secretaría, contabilidad, dirección, sala de profesores y la biblioteca, el cableado estructurado de la red se encuentra con algunas deficiencias, motivo por el cual se recomienda dotar de los materiales necesarios para salvaguardar el buen funcionamiento de la red en la Extensión Universitaria de Zamora.

- Preparar y mejorar la red universitaria de Zamora con dispositivos, sistemas operativos y aplicaciones que estén realmente listos o en camino de cumplir las especificaciones de IPv6, sin descartar completamente las aplicaciones que son válidas en IPv4.

- Se recomienda a futuro el reemplazo paulatino de túneles y demás mecanismos utilizados por la migración nativa IPv6 empezando por el Campus de la UTPL para luego complementarlo con los Centros Asociados.

- Se recomienda además que se lleve a cabo a futuro la Implementación del presente proyecto de Tesis en las extensiones universitarias como proyecto piloto, para conllevar la tecnología a la par y usar las nuevas y/o mejoradas características que nos ofrece el Protocolo de la Nueva Generación IPv6.

- Apoyar e impulsar la difusión, investigación y formación sobre IPv6 en la sociedad académica de la UTPL, para fortalecer la cultura del aprovechamiento racional de esta nueva tecnología en el personal que coadyuva día a día al engrandecimiento de la UTPL.

- La implantación de este nuevo protocolo es una necesidad inmediata puesto que la mayoría de las aplicaciones y dispositivos que están siendo desarrollados hacen uso de las ventajas que éste les ofrece calidad de servicio (QoS) y clase de servicio (CoS).

- El uso de las tecnologías es un avance importante pero es necesario fomentar el desarrollo de la investigación, para ello cabe destacar la importancia de profundizar el conocimiento acerca de las relaciones existentes entre tecnologías y sistemas de gestión de la información, para iniciar el diseño de políticas y estrategias renovadas de modernización que

nos lleven al crecimiento y desarrollo de la UTPL, y a su vez que nos haga participes del dinamismo mundial en lo que respecta a la tecnología e investigación.

BIBLIOGRAFÍA Y REFERENCIAS:

[1] Internet World Stats, “Internet Usage Statistics”, 2008. Disponible en Web: http://www.internetworldstats.com/stats2.htm

[2] Internet Engineering Task Force, “IPv6”, 2008. Disponible en Web: http://www.ietf.org

[3] Marcelo Bagnulo, “Por qué IPv6”, 2007. Disponible en Web: http://www.lac.ipv6tf.org/

[4] Raúl Echeverría, “Anuncio agotamiento de direcciones IPv4”, 2007. Disponible en Web: http://www.lacnic.net/sp/anuncios/2007_agotamiento_ipv4.html

[5] Comisión Interamericana de Telecomunicaciones, “Especificación del IPv6”, 2006. Disponible en Web: http://www.citel.oas.org/newsletter/2006/septiembre/ipv6_e.asp

[6] Evelio Martínez, “IPv6: El protocolo del internet de la nueva generación”, 2004. Disponible en Web: http://www.eveliux.com/mx/index.php?option=com_content&task=view&id=18&Itemid=26

[7] Christian Huitima, “Protocolo de Internet versión 6”, 2007. Disponible en Web: http://www.codarec.frm.utn.edu.ar

[8] Scribd, “Integración de Redes”, 2007. Disponible en Web: http://www.scribd.com/doc/9566149/IPv6

[9] Miguel Luengo, “Introducción a IPv6”, 2007. Disponible en Web: http://www.cu.ipv6tf.org/pdf/ipv6-UNLP.PDF

[10] Montserrat Collado Rodríguez, “IPv6 el cercano gran desconocido”, 2007. Disponible en Web: http://www.evidalia.es/trucos/index_v2-261-11.html

[11] Damián Pérez Valdés, “Qué es el IPv6”, 2007. Disponible en Web: http://www.maestrosdelweb.com/principiantes/evolucionando-hacia-el-ipv6/

[12] Axel Ernesto Moreno, “IPv6 Interoperabilidad y Robustez”, 2004. Disponible en

Web:http://www.cs.cinvestav.mx/Estudiantes/TesisGraduados/2004/tesisAxelErnesto.pdf

[13] Derman Zepeda Vega, “Mecanismos de Transición IPv6”, 2007. Disponible en Web: http://www.renia.net.ni/documentos/FRIDA/metodos_transicion_ipv6.pdf

[14] TechNet, “Tráfico IPv6 entre nodos de sitios diferentes en Internet (6to4)”,2008. Disponible en Web: http://technet.microsoft.com/es-es/library/cc779985.aspx

[15] Christian Lazo R.”Servicio de Túneles IPv6”, 2007. Disponible en Web: http://www.lacnic.net/documentos/lacnicvii/Serv-tuneles-IPv6-FLIP6.pdf

[16] Jordi Palet, “Herramientas de Transición IPv6”, 2008. Disponible en Web: http://www.cuba.ipv6tf.org/talleripv6-2008/5.pdf

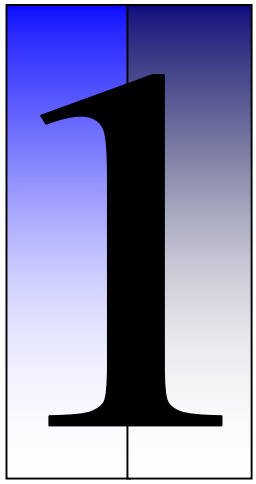
[17] Tech-Fap, “Comprender la convivencia y la migración”, 2007. Disponible en Web: http://www.tech-faq.com/lang/es/installing-ipv6.shtml&usg=ALkJrhg4Qre-6MJOLywbxUMonKx8l6-T2w.

[18] Wikipedia, “IPv6”, 2007. Disponible en Web: http://es.wikipedia.org/wiki/Ipv6

[19] Carlos Ralli Ucendo, “Mecanismos de Transición IPv4 - IPv6”, 2008. Disponible en Web: ww.cu.ipv6tf.org/pdf/carlos_ralli_transitiontutorial.pdf

[20] Evelio Martínez, “El protocolo de la nueva generación”, 2007. Disponible en Web: http://www.eveliux.com/mx/ipv6-el-protocolo-del-internet-de-la-nueva-generacion/page-3.php

ANEXOS



Anexo

Configuración de IPv6 en Windows y Linux

Configuración de IPv6 en Windows XP SP2:

En Windows XP, IPv6 ya está instalado pero es preciso habilitarlo. Para ello es necesario con privilegios de administrador realizar lo siguiente (Menú de Inicio – Ejecutar – CMD – Enter):

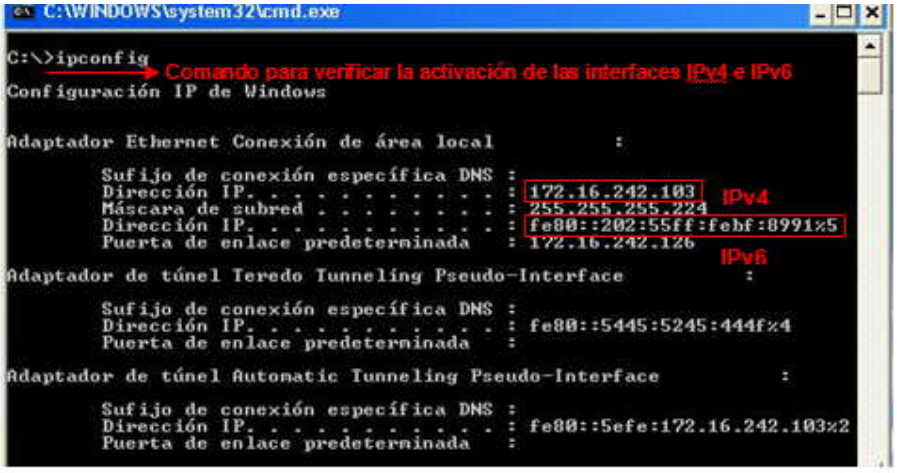
Activación de IPv6

Mediante el comando IPv6 install, se activa el protocolo IPv6, ya que en este sistema operativo Windows XP SP2 no viene activo el protocolo de la nueva generación, una vez que se ha instalado aparecerá un mensaje indicando que se ha configurado correctamente, pero en Windows Vista no sucede esto, en esta plataforma ya viene activado por defecto IPv6,

Una vez hecho esto debemos verificar que las interfaces de red ya cuentan con el protocolo IPv6 habilitado. Esto se logra de dos formas distintas:

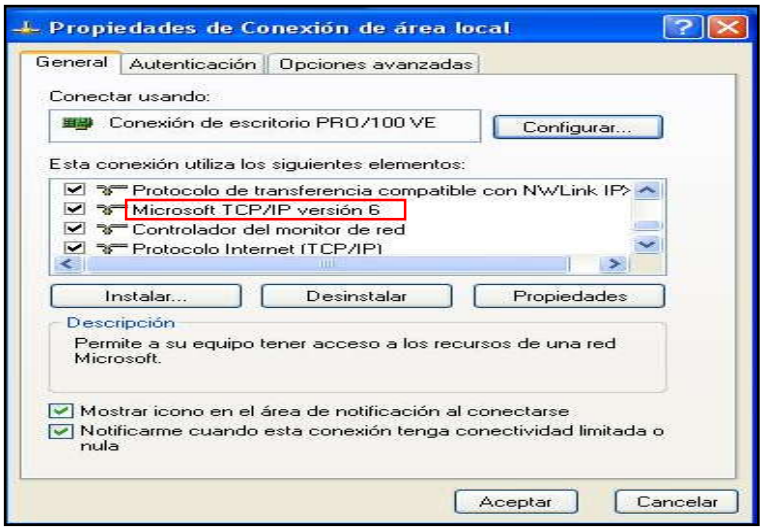
- Digitando: ***ipv6 if*** o a su vez Digitando: ***ipconfig***

En ambos casos debemos observar que todas las interfaces ya cuenten con IPv6 habilitado. Se mostrará la configuración y las direcciones IPv6 adquiridas (auto - configuradas) para cada interfaz de red existente, tal como se presenta en la figura siguiente:



Verificación de la activación de las interfaces

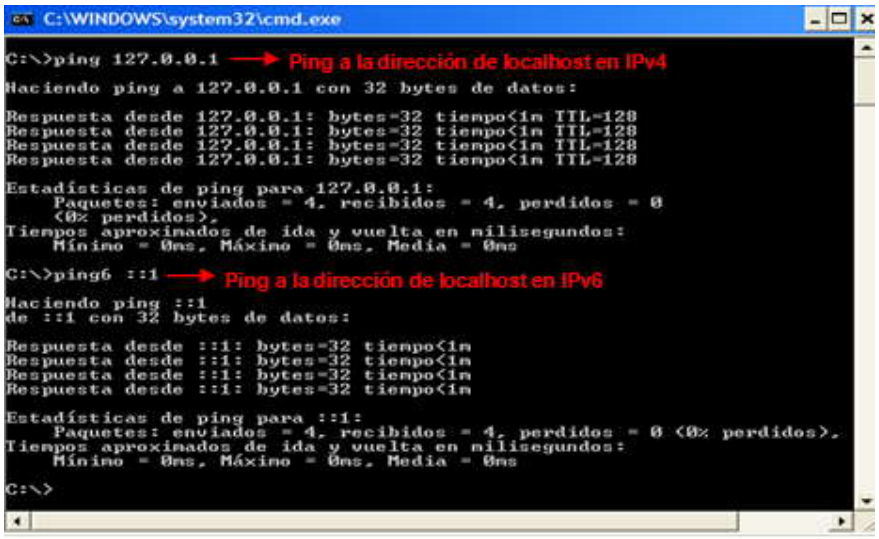
Otra opción para verificar si IPv6 está instalado es verificando desde la ventana de propiedades de red: (Conexiones de red - Conexión de área local - Propiedades).



Verificación de IPv6 en la ventana de Propiedades de Red

Desde la ventana de consola de Windows, se puede instalar/desinstalar IPv6. El protocolo de la nueva generación "***ipv6***" se puede utilizar para comprobar y configurar manualmente interfaces, direcciones y rutas en usuarios avanzados.

Además para comprobar el correcto funcionamiento de las pilas tanto en IPv4 como en IPv6, se hace ping a la dirección de loopback en ambos protocolos, tal como se muestra en la figura siguiente:



Ping de localhost en IPv4 e IPv6 (doble pila)

Configuración de IPv6 en Linux CentOS:

Primeramente se debe activar el soporte IPv6 en el Kernel, para lo cual se utiliza algunos comandos para editar los ficheros correspondientes, los que se detallan a continuación:

a. Digitar el comando: **vi /etc/sysconfig/network**, el comando **vi** en Linux permite abrir un fichero para luego editarlo; una vez ejecutado el comando anterior se abre el fichero y dentro de este se encuentran las siguiente variables: **NETWORKING** y **HOSTNAME**, las dos variables ya vienen con valores por defecto, por lo que no hay que modificarlas.

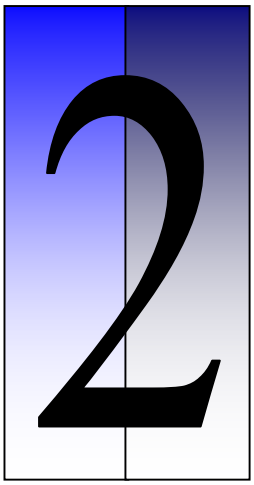
```
NETWORKING=yes
HOSTNAME=localhost.localdomain      #estacionz.ipv6.utpl.edu.ec/zamora
```

b. Luego se agrega una variable adicional a las anteriores, para poder escribir en el fichero y editarlo se presiona la tecla ***i*** o también la tecla ***insert*** y así podemos agregar, modificar y eliminar cualquier palabra dentro del archivo; seguidamente hay que ubicarse al final de la última variable y agregar lo siguiente: ***NETWORKING_IPv6=yes*.** Con ésta variable ya se activará IPv6 en Linux; entonces el fichero modificado quedará de la siguiente manera:

```
NETWORKING=yes
HOSTNAME= localhost.localdomain      #estacionz.ipv6.utpl.edu.ec/zamora
NETWORKING_IPV6=yes
```

c. Por último se procede a grabar los cambios realizados, de la siguiente manera: se presiona la tecla ***esc***, luego **shift** + la tecla de los ***dos puntos*** (al mismo tiempo) y finalmente se presiona la tecla ***x*** y un enter; de esta manera queda grabado el archivo. Para comprobar los cambios realizados se digita el siguiente comando: **cat /etc/sysconfig/network**. El resultado será el siguiente:

Verificación de los cambios realizados para IPv6 en el Kernel de Linux



Anexo 2

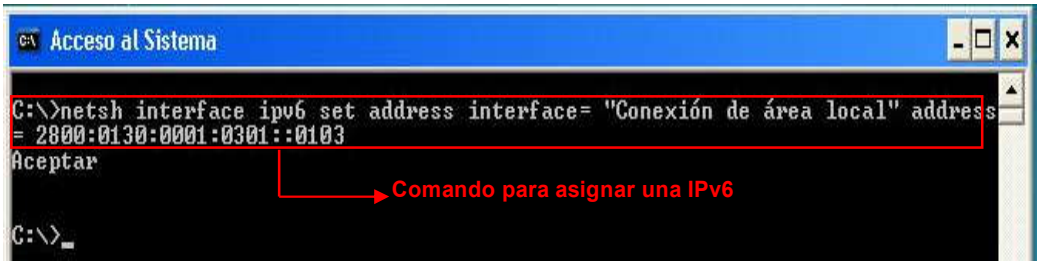
Configuración de Dual Stack en Windows y Linux

Configuración de Dual Stack (doble pila) en Windows SP2:

Una vez levantadas las interfaces tanto en la Pila IPv4 como en la Pila IPv6, se procede a realizar la configuración para asignar el direccionamiento en IPv6 tanto en Windows como en Linux y así contar ya con una dirección válida para IPv6, ya que en primera instancia al activar IPv6 se instala una dirección de host local (***fe80*::202:55ff:febf:8991%5**), la misma que no sirve para tener salida hacia el Internet, entonces debemos proceder a asignar una dirección válida en IPv6 de manera manual ya que es la forma como se ha realizado las pruebas de configuración para el presente proyecto de tesis, además de la forma manual de la asignación de direcciones IPv6, existe la forma dinámica DHCPv6 (Dinamic Host Control Protocol versión 6).

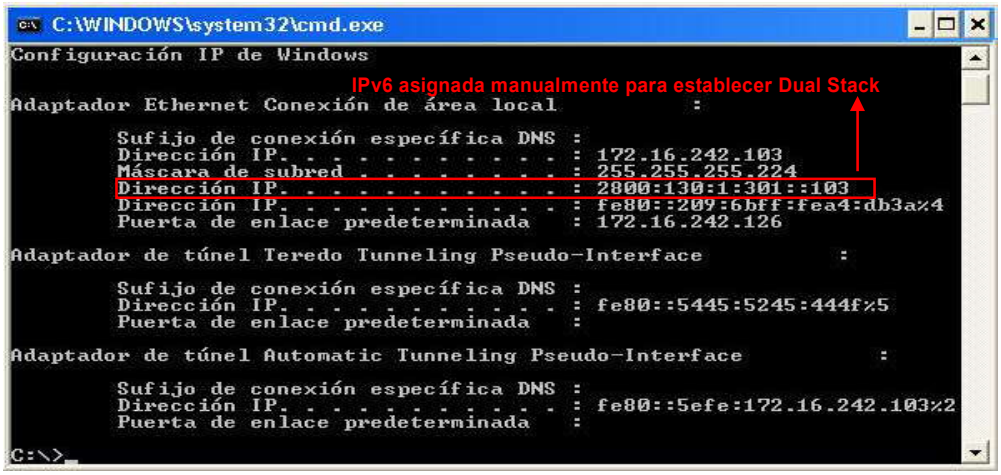
Establecimiento de Dual Stack (Doble Pila) en Windows:

Primeramente para asignar una dirección válida IPv6 para poder tener salida hacia el Internet, para realizar el transporte de datos en doble pila (Dual Stack – IPv4 e IPv6), se debe tener levantadas las interfaces de los dos protocolos, seguidamente se digita el comando para establecer una dirección válida en IPv6.



Asignación manual de una Dirección IPv6

Al asignar manualmente la dirección estática en IPv6, se podrá contar con un direccionamiento en Dual Stack, el cual servirá para realizar el transporte y envío de paquetes en doble pila (IPv4 e IPv6), así como también la salida hacia el Internet.



Asignación manual de una Dirección IPv6 válida

Configuración de Dual Stack (Doble Pila) en Linux:

Una vez activado IPv6, se debe asignar una dirección IPv6 estática a la interfaz, para poder tener doble pila, se lo realiza de la siguiente manera:

a. Editar el fichero correspondiente a la tarjeta de red, usar el siguiente comando: **vi *letc/sysconfig/network-scripts/ifcfg-eth0.***

b. Luego agregamos las siguientes variables:

IPV6INIT = yes (con esto iniciamos IPv6 en la tarjeta de red).

IPV6_AUTOCONF = no (con esto negamos que la tarjeta de red genere (una dirección IPv6 de manera automática).

IPV6ADDR = *2800:0130:0001:0301::0102* (con esto se asigna de manera estática una dirección IPv6 a la tarjeta de red).

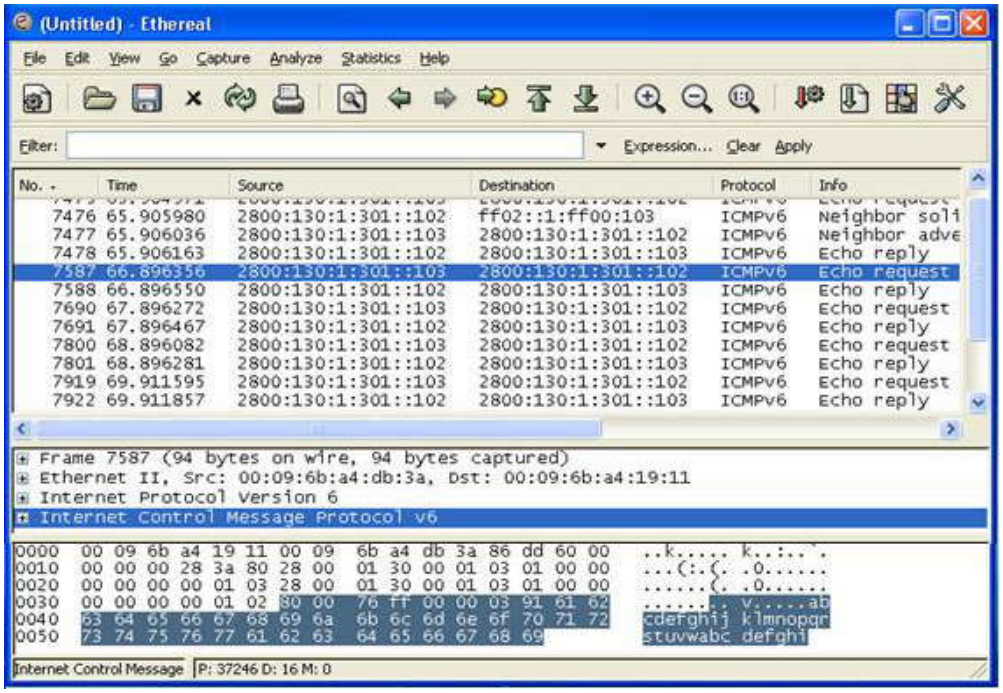
c. Finalmente se guarda los cambios en el fichero. El archivo ya editado debe ser parecido a la imagen presentada a continuación:

DEVICE=eth0	#identificador del dispositivo de red
HWADDR=00:09:6B:A4:19:11	#dirección MAC del dispositivo
ONBOOT=yes	#activar al inicio
TYPE=Ethernet	#tipo del dispositivo
IPV6INIT=yes	#inicializa IPv6 en la Interfase
IPV6_AUTOCONF=no	#deshabilita las técnicas de autoconfiguración
IPV6ADDR=2800:0130:0001:0301::0102	#asigna una dirección IPv6 a la tarjeta

NOTA: *En la imagen reciente anterior, todo lo que esta a la derecha del símbolo # es un comentario.*

d. Finalmente se reinicia los servicios de red con el comando: **service network restart** y se digita el comando **ifconfig,** y luego la dirección IPv6 debe estar configurada, se reinicia la máquina y la dirección no debe desaparecer, ya que se guardará los cambios en el registro del sistema.

Una vez realizada las configuraciones, tanto en Linux como en Windows, en Dual Stack (doble pila), podemos ya tener el doble direccionamiento, el cual es el propósito del presente proyecto de tesis, para lo cual se presentan las siguientes imágenes capturadas con el software ***Ethereal,*** el cual es un programa para realizar capturas de paquetes de una red:

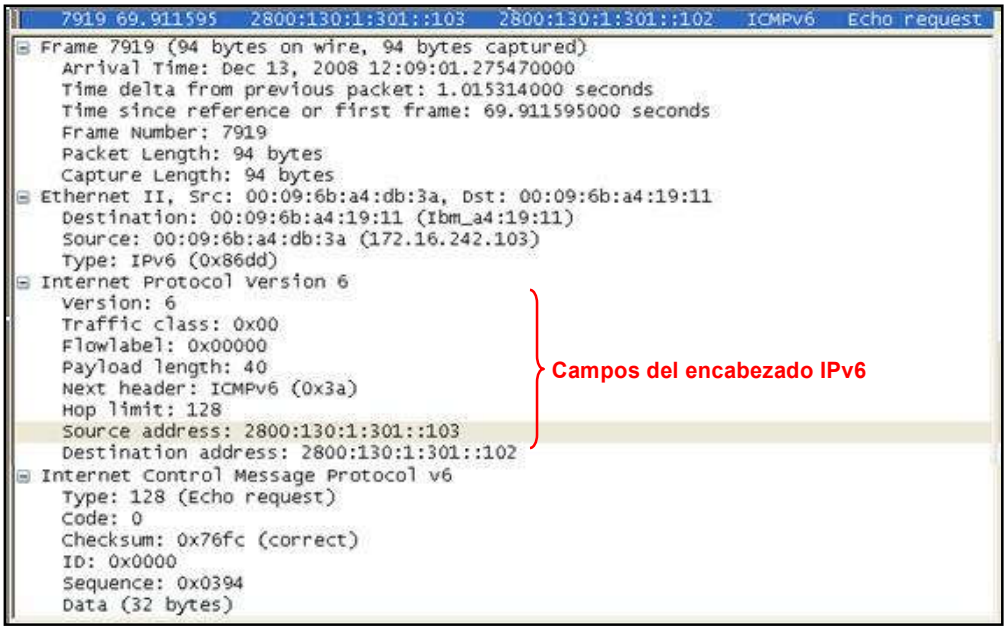


Captura de datagramas en IPv6

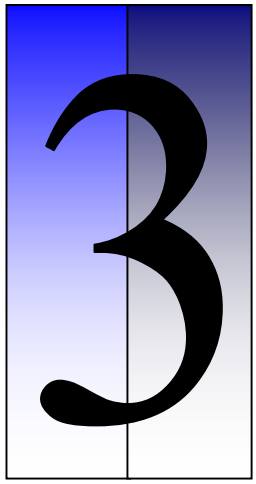
La estructura de un paquete IPv6, se presenta en la figura 24, la cual nos presenta los 8 campos con los que cuenta el encabezado del protocolo de la Nueva Generación IPv6, los cuales son:

- Versión: 6

- Traffic class: 0x00
- Flow label: 0x00000
- Payload: 40
- Next header: ICMPv6 (0x3a)
- Hop limit: 128
- Source address: 2800:0130:0001:0301::0103 (IPv6 orígen)
- Destination address: 2800:0130:0001:0301::0102 (IPv6 destino)



Estructura del encabezado de un datagrama en IPv6



Anexo

RFC`s relacionados con IPv4, IPv6 y Tecnologías de Redes

DESARROLLO DE POLÍTICAS DE SEGURIDAD EN LAS COMPUTADORAS:

RFC 1281 Directrices para la operación segura de Internet.

RFC 1457 Etiqueta del Marco de Seguridad para Internet.

RFC 2196 Manual de seguridad del sitio.

RFC 2323 IETF Identificación y Guía de seguridad.

RFC 2411 Seguridad IP Documento Plan de trabajo.

DISEÑO Y ADMINISTRACIÓN DE REDES:

RFC 817 Modularidad y Eficiencia en el Protocolo de Aplicación.

RFC 1070 Uso de Internet como una subred para la experimentación con la capa de red OSI.

RFC 1273 Un estudio de Medición de los cambios en el Nivel de accesibilidad en el Mundo TCP/IP.

RFC 1627 Red 10 consideran perjudiciales (Algunas prácticas no deben ser codificadas).

RFC 1052 IAB Recomendaciones para el Desarrollo de las Normas de gestión de la Red de Internet.

RFC 1065 Identificación de estructura y de Información de Gestión para TCP/IP-based internets para TCP / IP basada en Internet.

RFC 1466 Directrices para la Gestión de espacio de direcciones IP.

RFC 1631 El Traductor de direcciones de red IP (NAT).

RFC 1715 El H Ratio de Eficiencia para la Asignación de direcciones.

RFC 1881 Dirección de Gestión de asignación de IPv6.

RFC 1916 Renumeración empresa: experiencia y Solicitud de Información.

RFC 1933 Mecanismos de transición para Hosts y Routers IPv6.

RFC 1958 Principios de la arquitectura de Internet.

RFC 2063 Medición de flujo de tráfico: Arquitectura.

RFC 2064 Medición de flujo de tráfico: Medidor MIB.

RFC 2212 Especificación de la Garantía de Calidad de Servicio.

RFC 2330 Marco de la propiedad intelectual del rendimiento.

RFC 2386 Un marco para QoS basado en enrutamiento en Internet.

RFC 2391 Compartir la carga utilizando Traducción de direcciones de red IP (LSNAT).

RFC 2458 Hacia la PSTN / Internet Interconexión de redes - Pre-PINT Implementaciones.

RFC 2549 IP sobre aviar Carriers con Calidad de Servicio.

RFC 2667 IP Túnel MIB.

RFC 2709 Modelo de seguridad con IPsec modo túnel para dominios NAT.

FIREWALLS: FILTRADO DE PAQUETES Y MANEJO DE PROXY:

RFC 1579 Firewall-Friendly FTP.

RFC 1919 IP clásicas versus IP proxies transparentes.

RFC 2267 Red de filtrado de ingreso:La derrota de los ataques de denegación de servicio que emplean Origen Dirección IP spoofing.

RFC 2356 Sun SKIP transversal de Firewall para Mobile IP.

RFC 2588 IP Multicast y Firewalls.

RFC 2647 Terminología de la evaluación comparativa de rendimiento del Firewall.

REDES PRIVADAS VIRTUALES (VPN'S):

RFC 2547 Protocolo BGP/MPLS y Red Privada Virtual (VPN).

PROBLEMAS Y ESTÁNDARES DE PROTOCOLOS:

RFC 768 Protocolo de datagrama de usuario.

RFC 793 Protocolo de control de transmisión.

RFC 1002 Protocolo Estándar de Servicio NetBIOS sobre TCP / UDP Transportes: conceptos y métodos.

RFC1108 Departamento de Defensa de EE.UU. Seguridad para el Protocolo de Internet.

RFC1132 Un estándar para la transmisión de paquetes a través de IPX 802,2 Redes.

RFC1171 Conexión punto a punto del Protocolo para la Transmisión Multi-Protocolo de datagramas.

RFC 1180 Un Tutorial de TCP/IP.

RFC 1234 Tráfico IPX a través del túnel de IP Networks.

RFC 1241 Plan para una encapsulación del Protocolo de Internet: Versión 1.

RFC 1326 Encapsulación mutua considerados peligrosos.

RFC 1337 Tiempo-Espera Asesinato Riesgos en TCP.

RFC 1349 Tipo de servicio del protocolo de Internet Suite.

RFC 1362 Novell IPX en varios medios de comunicación WAN (IPXWAN).

RFC 1613 Cisco Systems X.25 a través de TCP (XOT).

RFC 1634 Novell IPX en varios medios de comunicación WAN (IPXWAN).

RFC 1853 IP en IP Tunneling.

RFC 1858 Consideraciones de seguridad para el filtrado de fragmentos IP.

RFC 2003 IP Encapsulation within IP.

RFC 2018 TCP Selective Acknowledgment Options.

RFC 2393 IP Payload Compression Protocol (IPComp).

RFC 2394 IP Payload Compression Using DEFLATE.

RFC 2395 IP Payload Compression Using LZS.

RFC 2401 Security Architecture for the Internet Protocol.

RFC 2460 Internet Protocol, Version 6 (IPv6) Specification.

RFC 2473 Generic Packet Tunneling in IPv6 Specification.

RFC 2521 ICMP Security Failures Messages.

RFC 2577 FTP Security Considerations.

RFC 2637 Point-to-Point Tunneling Protocol (PPTP).

ADMINISTRACIÓN DE LLAVES (PÚBLICAS - PRIVADAS) Y ENCRIPTADO:

RFC 1170 Public Key Standards and Licenses.

RFC 1321 The MD5 Message-Digest Algorithm.

RFC 1750 Randomness Recommendations for Security.

RFC 1810 Report on MD5 Performance.

RFC 1828 IP Authentication using Keyed MD5.

RFC 1829 The ESP DES-CBC Transform.

RFC 1851 The ESP Triple DES Transform.

RFC 1948 Defending Against Sequence Number Attacks.

RFC 1949 Scalable Multicast Key Distribution.

RFC 2040 The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms.

RFC 2085 HMAC-MD5 IP Authentication with Replay Prevention.

RFC 2093 Group Key Management Protocol (GKMP) Specification.

RFC 2094 Group Key Management Protocol (GKMP) Architecture.

RFC 2144 The CAST-128 Encryption Algorithm.

RFC 2202 Test Cases for HMAC-MD5 and HMAC-SHA-1.

RFC 2268 A Description of the RC2(r) Encryption Algorithm.

RFC 2314 PKCS #10: Certification Request Syntax Version 1.5

RFC 2315 PKCS #7: Cryptographic Message Syntax Version 1.5.

RFC 2367 PF_KEY Key Management API, Version 2.

RFC 2403 The Use of HMAC-MD5-96 within ESP and AH.

RFC 2404 The Use of HMAC-SHA-1-96 within ESP and AH.

RFC 2405 The ESP DES-CBC Cipher Algorithm With Explicit IV.

RFC 2406 IP Encapsulating Security Payload (ESP)

RFC 2407 The Internet IP Security Domain of Interpretation for ISAKMP.

RFC 2408 Internet Security Association and Key Management Protocol (ISAKMP).

RFC 2409 The Internet Key Exchange (IKE).

RFC 2410 The NULL Encryption Algorithm and Its Use With IPsec.

RFC 2412 The OAKLEY Key Determination Protocol.

RFC 2419 The PPP DES Encryption Protocol, Version 2 (DESE-bis).

RFC 2420 The PPP Triple-DES Encryption Protocol (3DESE).

RFC 2437 PKCS #1: RSA Cryptography Specifications Version 2.0.

RFC 2451 The ESP CBC-Mode Cipher Algorithms.

RFC 2510 Internet X.509 Public Key Infrastructure Certificate Management Protocols.

RFC 2511 Internet X.509 Certificate Request Message Format.

RFC 2522 Photuris: Session-Key Management Protocol.

RFC 2527 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

RFC 2559 Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2.

RFC 2585 Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP.

RFC 2587 Internet X.509 Public Key Infrastructure LDAPv2 Schema.

RFC 2612 The CAST-256 Encryption Algorithm.

RFC 2631 Diffie-Hellman Key Agreement Method.

RFC 2661 Layer Two Tunneling Protocol "L2TP".

RFC 2692 SPKI Requirements.

RFC 2693 SPKI Certificate Theory.

JUICIOS DE AUDITORIA, CASOS FORENSES Y RESPUESTA DE INCIDENTES EN TOPOLOGÍAS DE RED:

RFC 2350 Expectations for Computer Security Incident Response.

AUTENTICACIÓN:

RFC 1334 PPP Authentication Protocols.

RFC 1507 DASS Distributed Authentication Security Service.

RFC 1510 The Kerberos Network Authentication Service (V5).

RFC 1511 Common Authentication Technology Overview.

RFC 1852 IP Authentication using Keyed SHA.

RFC 2138 Remote Authentication Dial In User Service (RADIUS).

RFC 2139 RADIUS Accounting.

RFC 2402 IP Authentication Header.

RFC 2433 Microsoft PPP CHAP Extensions.

RFC 2548 Microsoft Vendor-specific RADIUS Attributes.

RFC 2618 RADIUS Authentication Client MIB.

RFC 2619 RADIUS Authentication Server MIB.

RFC 2620 RADIUS Accounting Client MIB.

RFC 2621 RADIUS Accounting Server MIB.

RFC 2712 Addition of Kerberos Cipher Suites to Transport Layer Security (TLS).

MEJORAS Y AVANCES DE LOS ESTÁNDARES:

RFC 1071 Computing the Internet Checksum.

RFC 1072 TCP Extensions for Long-Delay Paths.

RFC 1077 Critical Issues in High Bandwidth Networking.

RFC 1158 Management Information Base for Network Management of TCP/IP-based internets: MIB-II.

RFC 1335 A Two-Tier Address Structure for the Internet: A Solution to the Problem of Address Space Exhaustion.

RFC 1038 Draft Revised IP Security Option.

RFC 3195 Reliable Delivery for syslog.

PROBLEMAS DE RUTEO Y ESTÁNDAR DE PROTOCOLOLOS:

RFC 1164 Application of the Border Gateway Protocol in the Internet.

RFC 1370 Applicability Statement for OSPF.

RFC 1403 BGP OSPF Interaction.

RFC 1454 Comparison of Proposals for Next Version of IP.

RFC 1701 Generic Routing Encapsulation (GRE).

RFC 1702 Generic Routing Encapsulation over IPv4 networks.

RFC 1745 BGP4/IDRP for IP---OSPF Interaction.

RFC 1772 Application of the Border Gateway Protocol in the Internet.

RFC 1773 Experience with the BGP-4 protocol.

RFC 1774 Análisis del Protocolo BGP-4.

RFC 1940 Source Demand Routing: Packet Format and Forwarding Specification (Version 1).

RFC 2082 RIP-2 MD5 Authentication.

RFC 2154 OSPF with Digital Signatures.

RFC 2281 Cisco Hot Standby Router Protocol (HSRP).

RFC 2328 OSPF Version 2.

RFC 2329 OSPF Standardization Report.

RFC 2385 Protection of BGP Sessions via the TCP MD5 Signature Option.

RFC 2560 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP.

RFC 2676 QoS Routing Mechanisms and OSPF Extensions.

PROBLEMAS DE SEGURIDAD DEL DNS (DOMAIN NAME SERVICE):

RFC 1536 Common DNS Implementation Errors and Suggested Fixes.

RFC 1537 Common DNS Data File Configuration Errors.

RFC 2230 Key Exchange Delegation Record for the DNS.

RFC 2541 DNS Security Operational Considerations.

MISCELANEOS:

RFC 1336 Who's Who in the Internet Biographies of IAB, IESG and IRSG Members.

RFC 1760 The S/KEY One-Time Password System.

RFC 2084 Considerations for Web Transaction Security.

RFC 2105 Cisco Systems' Tag Switching Architecture Overview.

RFC 2151 A Primer On Internet and TCP/IP Tools and Utilities.

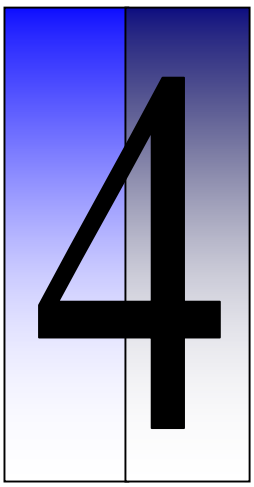
RFC 2179 Network Security For Trade Shows.

RFC 2289 A One-Time Password System.

RFC 2444 The One-Time-Password SASL Mechanism.

RFC 2478 The Simple and Protected GSS-API Negotiation Mechanism.

RFC 2479 Independent Data Unit Protection Generic Security Service Application Program Interface (IDUP-GSS-API).



Presupuesto y Cotizaciones de los Equipos para la RED

Anexo

COTIZACIÓN DE EQUIPOS

La cotización de los equipos propuestos para el diseño de la propuesta del presente proyecto de tesis se la realizó previa investigación en la página Web siguiente:

Enlace Web de la cotización de los equipos necesarios para la RED: http://www.andean-trade.com/index.php?page=shop.browse&category_id=1&option=com_virtuemart&Itemid=1

En esta página se encuentra la valoración de los equipos propuestos para la implementación de la transición, a continuación se detallan las características y los precios de los equipos:

Cantidad	Equipo	Precio Unitario USD.	Precio Total USD.
2	Router Cisco 3660	$. 3.950	$. 7,900
1	Switch Catalyst 2950	$. 4.120	$. 4,100

De acuerdo a la cotización de los equipos recomendados, la inversión que se deberá realizar para la adquisición de los equipos para la Topología de Red propuesta para realizar la Transición será por un monto total a: ***USD. 12.000 Dólares Americanos*.**

INDICE DE FIGURAS

INDICE DE TABLAS