**UNIVERSIDAD NACIONAL DE CHIMBORAZO**

**FACULTAD DE INGENIERIA**

**ESCUELA DE ELECTRONICA Y TELECOMUNICACIONES**

**TRABAJO DE GRADO PREVIO A LA OBTENCION DEL TITULO DE:**

**"INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES"**

**MODALIDAD: TESIS**

**Titulo:**

# "IMPLEMENTACIÓN DEL SERVICIO DNS (SISTEMA DE NOMBRES DE DOMINIO) Y DIRECCIONAMIENTO INTERNO SOBRE EL PROTOCOLO IPv6 EN LA UNACH"

**Autor: (es)**

**GEOVANNA NATALIA MORENO FERNANDEZ**

**CRISTINA ALEJANDRA OROZCO CAZCO**

**Director de Tesis:**

**ING. DANIEL SANTILLÁN**

**RIOBAMBA**

**2011-2012**

## CALIFICACIÓN

**Los miembros del tribunal, luego de haber receptado la Defensa de trabajo escrito, hemos determinado la siguiente calificación.**

## CALIFICACIONES DEL TRIBUNAL

| | Números | Letras |
|---|---|---|
| **Presidente del Tribunal** | | |
| **Director de Tesis** | | |
| **Miembro del Tribunal** | | |
| **PROMEDIO FINAL** | | |

**Para constancia de lo expuesto firman:**

| | |
|---|---|
| ---------- | ---------- |
| **Presidente (Ing. Yesenia Cevallos)** | **Firma** |
| ---------- | ---------- |
| **Director (Ing. Daniel Santillán)** | **Firma** |
| ---------- | ---------- |
| **Miembro (Ing. Javier Haro)** | **Firma** |

**DERECHO DE AUTOR**

## DEDICATORIA

*Quiero dedicar este proyecto a Dios en primer lugar por haberme permitido llegar hasta este punto y haberme dado salud para lograr mis objetivos, además de su infinita bondad y amor.*

*A mis padres y hermanos por haberme apoyado en todo momento, por sus consejos, sus valores, por la motivación constante que me ha permitido ser una persona de bien, pero más que nada, por su amor y por los ejemplos de perseverancia y constancia que los caracterizan para salir adelante.*

*Geovanna M.*

## DEDICATORIA

*Este trabajo se lo dedico a los seres que me dieron la vida que son quienes me brindaron su apoyo incondicional, su cariño y comprensión, a mis queridos hermanos por ser un ejemplo de constante esfuerzo y sacrificio, y especialmente a Dios por permitirme conocer a tantos seres maravillosos quienes estuvieron junto a mí para poder cumplir este gran sueño.*

*Cristina O*.

## AGRADECIMIENTO

*Este trabajo es la muestra de haber llegado a la etapa final de nuestra vida universitaria. Etapa en la que principalmente agradecemos a Dios y a las diversas personas que nos han influenciado positivamente a lo largo de estos años.*

*A nuestras familias y en especial a nuestros padres y hermanos, por apoyarnos y alentarnos en todas las decisiones que hemos tomado.*

*A todos nuestros amigos y amigas que tuvimos la fortuna de conocer durante nuestro paso por esta Universidad.*

*A todos los profesores que nos guiaron y nos impartieron sus conocimientos, en especial al Ing. Javier Haro por dedicarnos su tiempo y paciencia durante la ejecución de este trabajo.*

*Geovanna Moreno*

*Cristina Orozco*

# INDICE

## INDICE GENERAL

CAPITULO II

**INDICE DE TABLAS**

**INDICE DE FIGURAS**

# RESUMEN

El presente trabajo tiene como objetivo la implementación de los servicios WEB, DNS y el direccionamiento interno sobre el protocolo IPv6, revisando su topología de red actual y los cambios necesarios para la transición de Ipv4 a IPv6 y así brindar dicho servicio a la comunidad universitaria

Hoy en día, IPv6 es el nuevo protocolo de telecomunicaciones que está en pleno desarrollo, el cual traerá grandes beneficios. La implementación se realizó mediante el mecanismo de transición Dual Stack o Doble Pila, es decir, permite tener dos pilas: Pila IPv4 e IPv6 en un host.

IPv6 ofrece mayor espacio de direcciones, cambia de 32 a 128 bits, para soportar mayores niveles de jerarquías de direccionamiento, con direcciones unicast, multicast y anycast, es decir que broadcast no existe; tiene un formato de cabecera más flexible que en IPv4 lo que facilita que los routers procesen los datagramas de manera más rápida y mejore la velocidad.

Con la implementación del mecanismo Dual Stack se logró que los servicios trabajen con IPv4 e IPv6, sin crear impacto notable para los usuarios, debido a que trabaja de manera transparente, facilitando el cambio de red sin perder conectividad lo que permite mejorar la calidad de servicio (QoS).

# ACRÓNIMOS

**ARP:** Protocolo de Resolución de Direcciones (Address Resolution Protocol).

**ARPA:** Agencia de Programas Avanzados de Investigación.

**BIND:** Berkeley Internet Name Domain.

**CEDIA:** Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado.

**DHCP:** Protocolo de Configuración Dinámica de Host (Dynamic Host Configuration Protocol).

**DNS:** Sistema de Nombres de Dominio (Domain Name System)

**DoD:** Departamento de Defensa de los Estados Unidos.

**HTTP:** Protocolo de Transferencia de Hipertexto

**ICMP:** Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol).

**IGMP:** Protocolo de Gestión de Grupos en Internet

**IP:** Protocolo de Internet.

**IPV4:** Protocolo de Internet versión 4 (Internet Protocol version 4).

**IPV6:** Protocolo de Internet versión 6 (Internet Protocol version 6).

**ISP:** Proveedor de Servicios de Internet **(**Internet Service Provider).

**LAN:** Red de Area Local (Local Area Network).

**NAT:** Traducción de Dirección **(**Network Address Translation).

**OSI:** Modelo de Interconexión de Sistemas Abiertos (Open System Interconnection).

**QoS:** Calidad de Servicio.

**RSVP:** Protocolo de reserva de recursos (Resource Reservation Setup Protocol).

**SSH:** Secure Shell.

**TCP:** Protocolo de Control de Transmisión (Transmission Control Protocol).

**TTL:** Time To Live.

**UDP:** Protocolo de Data Grama de Usuario

**WEB:** World Wide Web (WWW).

# CAPITULO I

## 1. ANTECEDENTES

### 1.1 INTRODUCCIÓN

El protocolo IP fue desarrollado en 1973 junto con el protocolo TCP, como parte de un proyecto patrocinado por la Agencia de Programas Avanzados de Investigación (ARPA), del Departamento de Defensa de los Estados Unidos (DoD) [1]. El protocolo de internet fue diseñado como un protocolo de bajo costo. Dicho protocolo provee sólo las funciones necesarias para enviar un paquete desde un origen a un destino a través de un sistema interconectado de redes. El protocolo IP no fue diseñado para rastrear ni administrar el flujo de paquetes; estas funciones son realizadas por otros protocolos en otras capas.

Usualmente a IP se le denomina capa de internet del modelo TCP/IP. El objetivo de dicha capa es enviar paquetes desde un dispositivo utilizando el protocolo correcto que opera en esta capa, en la misma que se determina la mejor ruta y la comunicación de paquetes. En la capa de Internet de TCP/IP operan varios protocolos como IP, ICMP, ARP, RARP.

Existen 2 versiones del protocolo IP a nivel de capa de internet del Modelo TCP/IP que actualmente están siendo usadas; la versión 4 (IPv4) y la versión 6 (IPv6) los mismos que son los protocolos de transporte de datos de la capa 2 más ampliamente utilizado. Esta última fue desarrollada debido a la gran masificación

[1] Fuente: CLEVELAND Chris, Academia de Networking de Cisco Systems, Cisco “Guía del Primer Ano CCNA 1 y 2”, Tercera Edición, Editorial Pearson Educacion, S.A. Madrid, 2004. Pág. 347

que ha tenido el internet en el mundo global provocando el agotamiento de direcciones IPv4 el mismo que será implementado en la UNACH.

## 1.2 PLANTEAMIENO Y FORMULACIÓN DEL PROBLEMA

Los días del protocolo IP **Internet Protocol** (en español Protocolo de Internet) en su formato actual (IPv4) están contados. El crecimiento exponencial de Internet está llevando hacia el agotamiento de las direcciones IPv4, es decir a la progresiva merma de la cantidad de direcciones IPv4 disponibles. Es por esto que las poco más de cuatro mil millones de direcciones en todo el mundo que brinda IPv4[2] se han vuelto insuficientes para el crecimiento mundial. El hecho de que no haya suficiente espacio de direccionamiento con IPv4 está ocasionando que muchos países, no sólo Europa que se quedo sin direcciones, sino también países como Japón y los países de África y Latinoamérica tengan restricciones en el acceso a Internet[3].

El aumento drástico de la demanda de las limitadas direcciones de 32 bits conlleva a la saturación del espacio de direcciones, limita el crecimiento de internet, obstaculiza el uso de internet a nuevos usuarios.

En este proyecto se analizarán diferentes problemas, uno de ellos es verificar si la infraestructura de red con la que cuenta la UNACH si posee con los equipos de interconectividad necesarios para adaptarse a los nuevos cambios de tecnología de comunicación en este caso la implementación del nuevo protocolo del internet IPv6, mediante una transición de IPv4 a IPv6.

Cabe plantearse algunas preguntas, a las cuales daremos respuesta durante la ejecución del presente trabajo:

---

[2] Fuente: VERA Xiomara; Diseño de la transición de direcciones IPv4 a IPv6 en la Extensión Universitaria de Zamora; Ecuador 2009. http://www.cepra.utpl.edu.ec.pdf

[3] Fuente: www.wikipedia.com/direccionamientoipv4

¿Existen las condiciones técnicas necesarias para que se pueda implementar esta tecnología?, ¿Cuáles son los aspectos que se deben considerar?, ¿Cómo contribuirá la implementación del servicio DNS y direccionamiento interno sobre el protocolo IPv6 en la UNACH?

## 1.3 JUSTIFICACIÓN DEL PROBLEMA

En los últimos años las comunicaciones y la electrónica se han convertido en herramientas, que facilitan la realización de diferentes actividades, por un lado las comunicaciones han evolucionado de tal manera que cumplen con su objetivo en casi todos los ámbitos, un ejemplo es el INTERNET y su uso masivo, dado que su implementación y su funcionamiento se realiza de una manera estandarizada, de fácil acceso y manejo, logrando así grandes avances y el soporte de una gran variedad de servicios.

El propósito de este trabajo es dar la pauta para un inicio de grandes cambios en la UNACH que posibilitará un gran crecimiento de la red, el mejoramiento de la calidad de conectividad entre dispositivos que actualmente trabajan con el protocolo IP versión 4 por IPV6 que es un protocolo más avanzado y amplio, con posibilidades de conexión y desarrollo.

En virtud de esto, vemos el extenso campo de aplicación y las ventajas que puede ofrecer la transición al protocolo IPv6. Nosotros como profesionales debemos desarrollar nuestras capacidades para adaptarnos a estos nuevos avances tecnológicos, por lo cual es necesario iniciar el camino hacia la implementación de estos.

## 1.4 OBJETIVOS

### 1.4.1 OBJETIVO GENERAL

- Implementar el servicio DNS y direccionamiento interno sobre el protocolo IPv6 en la UNACH.

### 1.4.2. OBJETIVOS ESPECÍFICOS

- Realizar un diagnóstico sobre todas las redes existentes en la UNACH.

- Configurar los dispositivos de interconexión con que cuenta la UNACH para que brinden soporte IPv6.

- Realizar la implementación del protocolo IPv6 en la UNACH y sus posteriores pruebas de funcionalidad.

## 1.5. LIMITACIONES

En este trabajo no se tendrá limitaciones a la implementación del protocolo IPv6 en cuanto a infraestructura tecnológica, ya que la UNACH actualmente cuenta con dispositivos de red que permitirán desarrollar este tema de investigación.

Por lo tanto podemos acotar que nuestra investigación brindará la posibilidad de implementar el servicio DNS y el direccionamiento sobre el protocolo IPv6 en la Universidad Nacional de Chimborazo.

## 1.6. METODOLOGÍA

A continuación se presenta la metodología para la elaboración de este trabajo. Se muestran aspectos como el tipo de investigación, las técnicas y procedimientos que fueron utilizados para llevar a cabo dicha implementación.

### 1.6.1. TIPO DE INVESTIGACIÓN

- El método hipotético-deductivo se aplicara debido a que a partir de un problema detectado se formulara una hipótesis que se espera confirmar con la experiencia.

A nuestra consideración el método más completo es el método HIPOTÉTICO-DEDUCTIVO ya que en él se plantea una hipótesis que se puede analizar deductiva o inductivamente y posteriormente comprobar experimentalmente, es decir que se busca que la parte teórica no pierda su sentido, por ello la teoría se relaciona posteriormente con la realidad.

Para realizar una investigación debemos tener en cuenta varios aspectos importantes como por ejemplo la cantidad de elementos del objeto de estudio, el total de información que podemos extraer de estos elementos, las características comunes entre ellos, y si queremos ser más específicos se utilizaría la inducción científica, entonces tomaremos en cuenta las causas y características necesarias que se relacionan con el objeto de estudio.

### 1.6.2. POBLACIÓN MUESTRA.

La población es el conjunto total de individuos, objetos o medidas que poseen algunas características comunes observables en un lugar y en un momento determinado, constituye el objeto de la investigación, de donde se extrae la información requerida para el estudio; es decir, en este caso para nuestro objetivo serán todos los Host existentes en la Universidad Nacional de Chimborazo.

Luego debemos seleccionar una porción representativa de la población que permita generalizar los resultados de una investigación previa. El objetivo principal de la selección de la muestra es extraer información que resulte imposible estudiar en la población porque esta incluye la totalidad. Por lo que tomamos como muestra a los 130 host del Edificio Administrativo.

### 1.6.3. HIPÓTESIS.

La implementación del protocolo IPv6 en la Universidad Nacional de Chimborazo contribuye a mejorar los servicios de red existentes.

### 1.6.4. OPERACIONALIZACIÓN DE LAS VARIABLES

- ✓ Variable Independiente
  IPv6
- ✓ Variable Dependiente
  Servicios de Red.

### 1.6.4.1. OPERACIONALIZACIÓN CONCEPTUAL

| VARIABLE | TIPO | DEFINICIÓN |
|---|---|---|
| IPv6 | INDEPENDIENTE | Es una versión del protocolo Internet Protocol (IP), diseñada para reemplazar a Internet Protocol versión 4 (IPv4). |
| SERVICIOS DE RED | DEPENDIENTE | Servicio de red es la creación de una red de trabajo en un ordenador. Generalmente los servicios de red son instalados en uno o más servidores para permitir el compartir recursos a computadoras clientes. |

**Tabla I Operacionalización Conceptual de la Hipótesis**

### 1.6.4.2. OPERACIONALIZACIÓN METODOLÓGICA.

| HIPOTESIS | VARIABLES | INDICADORES | INSTRUMENTOS |
|---|---|---|---|
| La implementación del protocolo IPv6 en la Universidad Nacional de Chimborazo contribuye a mejorar los servicios de red existentes. | IPv6 | Cantidad de Hosts, utilizando IPv6 | Informe del Servidor DHCP |
| | | Tiempo de Respuesta | Comando ping |
| | Servicios de Red | Número de Servicios IPv6 en Internet | http://www.mrp.net/IPv6_Survey.html<br><br>http://ipv6.cedia.org.ec/index.php/la-realidad |

**Tabla II Operacionalización Metodológica de la Hipótesis**

# CAPITULO II

## 2. ANALISIS ENTRE LOS PROTOCOLOS IPv4 E IPv6

### 2.1. IPv4

El protocolo de Internet (IP) es un protocolo no orientado a conexión usado para trasmitir datagramas a través de una red de paquetes conmutados, fue diseñado como un protocolo de bajo costo. Es el único protocolo de la capa de Internet del modelo TCP/IP que se utiliza para llevar datos de usuario a través de Internet. Sin embargo, la entrega del paquete sin conexión puede hacer que los paquetes lleguen al destino fuera de secuencia. Si los paquetes que no funcionan o están perdidos crean problemas para la aplicación que usa los datos, luego los servicios de las capas superiores tendrán que resolver estos inconvenientes.

El protocolo de Internet versión 4 (IPv4) es la cuarta iteración del protocolo IP y la primera versión en ser utilizada en ambientes de producción.[4] Es el protocolo dominante en Internet, provee funciones necesarias para entregar paquetes desde un nodo de origen a uno de destino a través de un sistema interconectado de redes. La capa de red debe proporcionar un mecanismo para direccionar estos dispositivos finales. Si las secciones individuales de datos deben dirigirse a un dispositivo final, este dispositivo debe tener una dirección única. En una red IPv4, cuando se agrega esta dirección a un dispositivo, al dispositivo se lo denomina host.

[4] Fuente: CLEVELAND Chris, Academia de Networking de Cisco Systems, Cisco "Guía del Primer Ano CCNA 1 y 2", Tercera Edición, Editorial Pearson Educacion, S.A. Madrid, 2004. Pág 351

IPv4 encapsula o empaqueta el datagrama o segmento de la capa de transporte para que la red pueda entregarlo a su host de destino. El protocolo no fue diseñado para rastrear ni administrar el flujo de paquetes. Estas funciones son realizadas por otros protocolos en las capas superiores.

La función de la capa de red es transportar los paquetes entre los hosts tratando de colocar la menor carga posible en la red. La capa mencionada anteriormente agrega un encabezado para que pueda enrutar los paquetes a través de redes complejas y lleguen al destino. El encabezado de un paquete IP no incluye los campos requeridos para la entrega confiable de datos. No hay acuses de recibo de entrega de paquetes. No hay control de error para datos. Tampoco hay forma de rastrear paquetes; por lo tanto, no existe la posibilidad de retransmitir paquetes.

Dentro de sus principales características se encuentran:

- Enrutamiento y direccionamiento: Provee una dirección única a cada dispositivo de una red de paquetes. IPv4 fue especialmente diseñado para facilitar el enrutamiento de paquetes a través de redes de diversa complejidad.

- Sin conexión: no establece conexión antes de enviar los paquetes de datos.

- Mejor esfuerzo: El protocolo IP provee un servicio de transmisión de paquetes no fiable (o de mejor esfuerzo). No usan encabezados que garanticen la entrega correcta de paquetes.

- Independiente de los medios: funciona sin importar los medios que transportan los datos.

### 2.1.1. CABECERA DEL PROTOCOLO IPv4

El formato del protocolo IPv4 del encabezado que viaja actualmente en cada paquete de datos de internet, se muestra en la figura 2.1

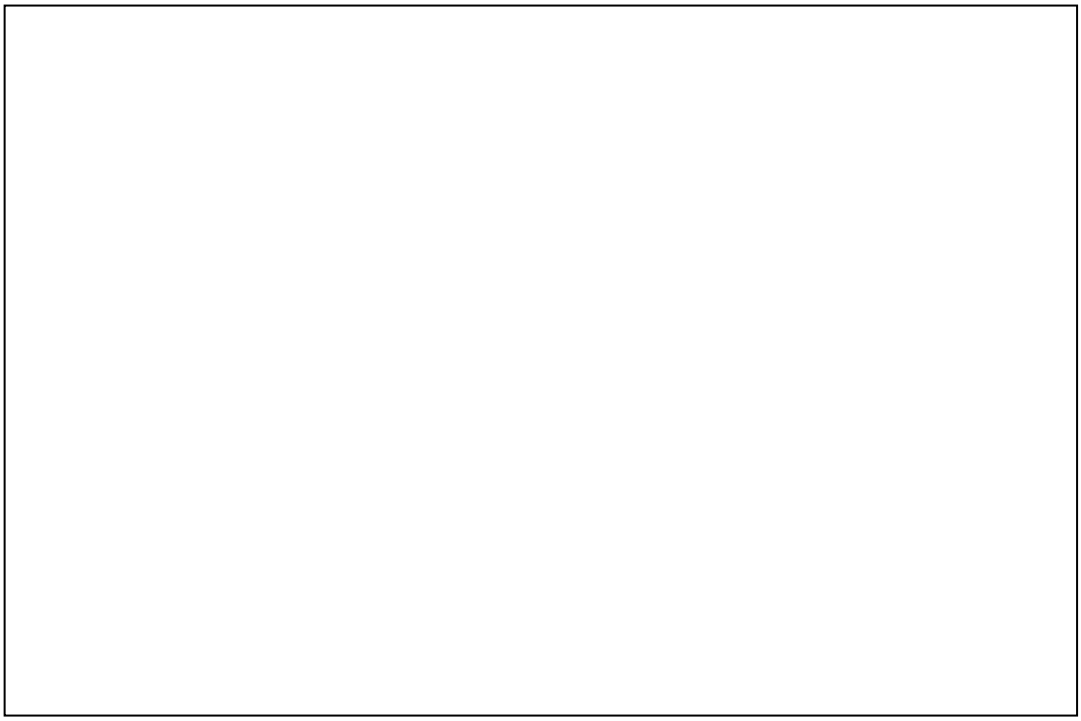


**FIGURA 2.1 FORMATO DE LA CABECERA DEL PROTOCOLO IPV4** [5]

### 2.1.1.1 DESCRIPCIÓN DE LA CABECERA DEL PROTOCOLO IPv4

| CAMPO | TAMAÑO | DESCRIPCIÓN |
|---|---|---|
| **Version** | 4 bits | «0100» indica versión 4. |
| **Tamaño de Cabecera (IHL)** | 4 bits | Longitud de la cabecera, en palabras de 32 bits. Su valor mínimo es de 5 para una cabecera correcta, y el máximo de 15. |

[5]Fuente: VERA Xiomara; Diseño de la transición de direcciones IPv4 a IPv6 en la Extensión Universitaria de Zamora; Ecuador 2009. http://www.cepra.utpl.edu.ec.pdf. pág 4

| | | |
|---|---|---|
| **Tipo de Servicio** | 8 bits | Indica una serie de parámetros sobre la calidad de servicio deseada durante el tránsito por una red. Algunas redes ofrecen prioridades de servicios, considerando determinado tipo de paquetes "más importantes" que otros (en particular estas redes solo admiten los paquetes con prioridad alta en momentos de sobrecarga). |
| **Longitud Total** | 16 bits | Es el tamaño total, en octetos, del datagrama, incluyendo el tamaño de la cabecera y el de los datos. El tamaño mínimo de los datagramas usados normalmente es de 576 octetos (64 de cabeceras y 512 de datos). Una máquina no debería enviar datagramas menores o mayores de ese tamaño a no ser que tenga la certeza de que van a ser aceptados por la máquina destino.<br><br>En caso de fragmentación este campo contendrá el tamaño del fragmento, no el del datagrama original. |
| **Identificación** | 16 bits | Identificador único del datagrama. Se utilizará, en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro. El originador del datagrama debe asegurar un valor único para la pareja origen-destino y el tipo de protocolo durante el tiempo que |

| | | |
|---|---|---|
| | | el datagrama pueda estar activo en la red. El valor asignado en este campo debe ir en formato de red. |
| **Indicador** | 8 bits | Actualmente utilizado sólo para especificar valores relativos a la fragmentación de paquetes:<br><br>bit **2**: Reservado; debe ser 0<br>bit **1**: **0** = Divisible, **1** = No Divisible (DF)<br>bit **0**: **0** = Último Fragmento, **1** = Fragmento Intermedio (le siguen más fragmentos) (MF)<br><br>La indicación de que un paquete es indivisible debe ser tenida en cuenta bajo cualquier circunstancia. Si el paquete necesitara ser fragmentado, no se enviará. |
| **Desplazamiento de Fragmentos** | 13 bits | En paquetes fragmentados indica la posición, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original. El primer paquete de una serie de fragmentos contendrá en este campo el valor 0. |
| **Tiempo de vida (TTL)** | 8 bits | Indica el máximo número de enrutadores que un paquete puede atravesar. Cada vez que algún nodo procesa este paquete disminuye su valor en 1 como mínimo, una unidad. Cuando llegue a ser 0, el |

| | | |
|---|---|---|
| | | paquete será descartado. |
| **Protocolo** | 8bits | Indica el protocolo de las capas superiores al que debe entregarse el paquete |
| **Checksum** | 16 bits | Suma de Contol de cabecera. Se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el Tiempo de Vida). |
| **Dirección IP de origen** | 32 bits | Dirección del nodo emisor |
| **Dirección IP de destino** | 32 bits | Dirección del nodo de destino, que puede ser un nodo final o un nodo intermedio. |

**TABLA III DESCRIPCIÓN DE LA CABECERA DEL PROTOCOLO IPV4**

### 2.1.2. DIRECCIONAMIENTO IPv4

En la versión 4 del protocolo IP, 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, como por ejemplo: 217.76.128.63. Cada dirección IP está formada por 32 bits agrupados en 4 conjuntos de 8 bits cada uno (octetos).

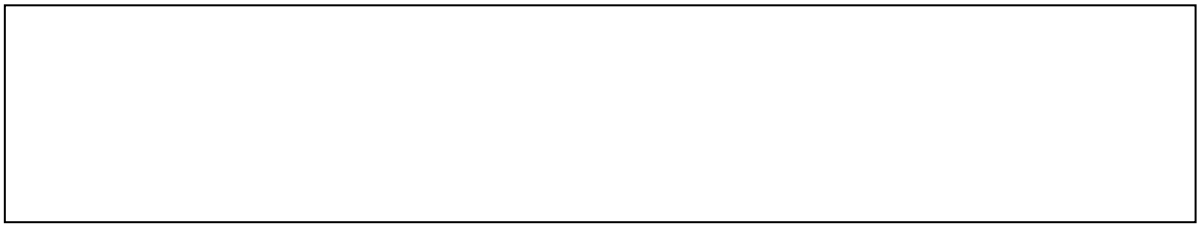


**FIGURA 2.2 FORMATO DE LAS DIRECCIONES IPV4 [6]**

[6] Fuente: VERA Xiomara; Diseño de la transición de direcciones IPv4 a IPv6 en la Extensión Universitaria de Zamora; Ecuador 2009. http://www.cepra.utpl.edu.ec.pdf. Pág 4

Cada red de una empresa tiene una dirección; los host 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.

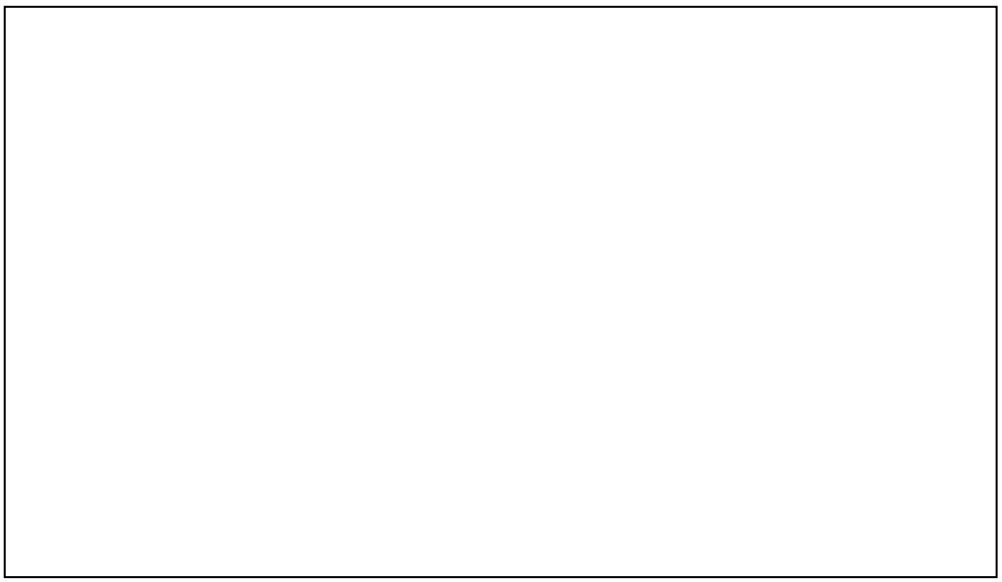


**FIGURA 2.3 ESQUEMA DE COMUNICACIÓN EN IPV4** [7]

### 2.1.3 TIPOS DE DIRECCIONES EN IPv4

IPv4 diferencia básicamente 3 tipos de direcciones. Públicas, Privadas y Reservadas.

- Las direcciones Públicas son aquellas que podemos usarlas para navegar.
- Las direcciones Privadas son aquellas que no podemos usar para navegar.
- Las direcciones Reservadas son direcciones que no deben usarse nunca salvo alguna circunstancia para la cual han sido reservadas.

[7] Fuente: VERA Xiomara; Diseño de la transición de direcciones IPv4 a IPv6 en la Extensión Universitaria de Zamora; Ecuador 2009. http://www.cepra.utpl.edu.ec/pdf. pág 5

### 2.1.3.1. DIRECCIONES PÚBLICAS

Las direcciones públicas son aquellas que son enrutables hacia internet, es decir aquellas con las cuales podemos tener acceso a internet.

Algunos ejemplos de direcciones públicas son:

**23.5.78.224 ----- 145.67.9.123 ----- 201.127.223.2**

Debemos tener en consideración que las direcciones **125.0.0.0** y **125.255.2555.255** son direcciones públicas, pero no son asignables a terminales. La primera es una dirección de red y la segunda una dirección de BROADCAST; ambas de la red **125.X.X.X**

### 2.1.3.2. DIRECCIONES PRIVADAS

Las direcciones privadas son aquellas que no podemos usar para enrutar hacia internet. Son direcciones útiles para ser usadas en redes de áreas locales (LANs) como es el caso entornos domésticos o corporativos. Hay mecanismos que permiten traducir direcciones privadas en públicas, es decir, los hosts en una red direccionada en forma privada pueden tener acceso a recursos a través de Internet. Este método se lo conoce como NAT el cual permite a los hosts de la red "pedir prestada", es decir, adquirir una dirección pública para comunicarse con redes externas. La traducción de dirección de red (NAT), pueden ser implementados en un dispositivo en un extremo de la red privada y los clientes de la mayoría de las aplicaciones pueden acceder a los servicios de Internet sin problemas evidentes.

Algunos ejemplos de direcciones privadas son:

**10.18.234.12 ----- 172.16.34.107 ----- 192.168.1.12**

Los siguientes rangos de direcciones están reservados para su uso privado:

- Rango de **10.0.0.0** a **10.255.255.255**
- Rango de **172.16.0.0** a **172.31.255.255**
- Rango de **192.168.0.0** a **192.168.255.255**

### 2.1.3.3. DIRECCIONES RESERVADAS

Las direcciones reservadas son grupos de direcciones que han quedado para un uso específico. Las más importantes son las siguientes:

- 0.0.0.0 (o la dirección .0 de cualquier subred). Esta es la dirección para referirse a la red
- 255.255.255.255 ( o la dirección .2555 de cualquier subred). Esta es la dirección de broadcast. Equivale a todos los terminales de red
- 127. X.X.X este es el rango de IPs de loopback. Son para referirnos a nosotros mismos (nuestra maquina). También llamadas de diagnostico.
- 127.0.0.1 (o local host). Es un caso particular de lo anterior. Es la más usada para referirnos a nuestra maquina de manera local

## 2.2. MASCARAS

En el principio de internet, las direcciones eran consideradas usando clases, se asumía una máscara implícita dependiendo de la clase de dirección. Estas clases son las siguientes:

- Clase A: **0.0.0.0** a **127.255.255.255** Mascara: **255.0.0.0** --- Broadcast **X.X.255.255**
- Clase B: **128.0.0.0** a **191.255.255.255** Mascara: **255.255.0.0** --- Broadcast **X.X.255.255**

- Clase C: **192.0.0.0** a **223.255.255.255** Mascara: **255.255.255.0** --- Broadcast **X.X.X.255**
- Clase D: **224.0.0.0** a **239.255.255.255** Dirección Multicast
- Clase E: **240.0.0.0** a **255.255.255.255** Dirección de Investigación

## 2.3. UNICAST, MULTICAST Y BROADCAST

- Un paquete UNICAST es aquel que va destinado a una sola IP de una red.
- Un paquete MULTICAST es aquel que va destinado a un conjunto de terminales de una red.
- Un paquete BROADCAST es aquel que va destinado a todos los terminales de una red.

## 2.4 IPv6

El protocolo IPv6 comenzó a desarrollarse en el año 1990, tras la primera voz de alerta sobre el posible agotamiento de direcciones IPv4. El protocolo IPv6 es considerado una evolución más que una revolución respecto al protocolo IPv4. **IPv6** al igual que IPv4 es el protocolo que se usa en la capa de Internet del Modelo TCP/IP

Se han mantenido los conceptos principales del protocolo, removiendo aquellas características de IPv4 que son poco utilizadas en la práctica. Se han añadido nuevas características que buscan solucionar los problemas existentes en el protocolo IPv4.

### 2.4.1 CARACTERISTICAS DEL PROTOCOLO IPv6

Dentro de las principales características de IPv6 se encuentran:

***Mayor capacidad de direccionamiento****:* en IPv6 el espacio de direccionamiento aumentó de 32 bits a 128 bits, permitiendo: niveles más específicos de agregación de direcciones, identificar una cantidad mucho mayor de dispositivos en la red e implementar mecanismos de autoconfiguración. También se mejoró la escalabilidad del enrutamiento *multicast* mediante la adición del campo "alcance" en la dirección *multicast*. También se definió un nuevo tipo de direcciones, las direcciones *anycast*

***Simplificación del formato del encabezado***: con el objetivo de reducir el costo de procesamiento de los paquetes en los routers, algunos campos del encabezado IPv4 se eliminaron o se convirtieron en opcionales

***Soporte para encabezados de extensión****:* las opciones dejaron de formar parte del encabezado base, permitiendo un enrutamiento más eficaz, límites menos rigurosos en cuanto al tamaño y la cantidad de opciones, y una mayor flexibilidad para la introducción de nuevas opciones en el futuro;

***Capacidad de identificar flujos de datos****:* se agregó un nuevo recurso que permite identificar paquetes que pertenecen a determinados flujos de tráfico que pueden requerir tratamientos especiales como mecanismos de QoS.

***Soporte para autenticación y privacidad****:* se especificaron encabezados de extensión capaces de proveer mecanismos de autenticación y garantizar la integridad y confidencialidad de los datos transmitidos.

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

***Nuevo protocolo para interactuar con vecinos:*** Este protocolo realiza funciones para IPv6 similares a las realizadas por ARP en IPV4. Es el encargado de descubrir

otros nodos en el enlace, realizar la resolución de direcciones IPv6 y direcciones MAC, encontrar los "routers" disponibles y mantener información actualizada sobre el estado de los caminos hacia otros nodos.

Una de sus mayores ventajas es que elimina la necesidad de los mensajes del tipo "BROADCAST".

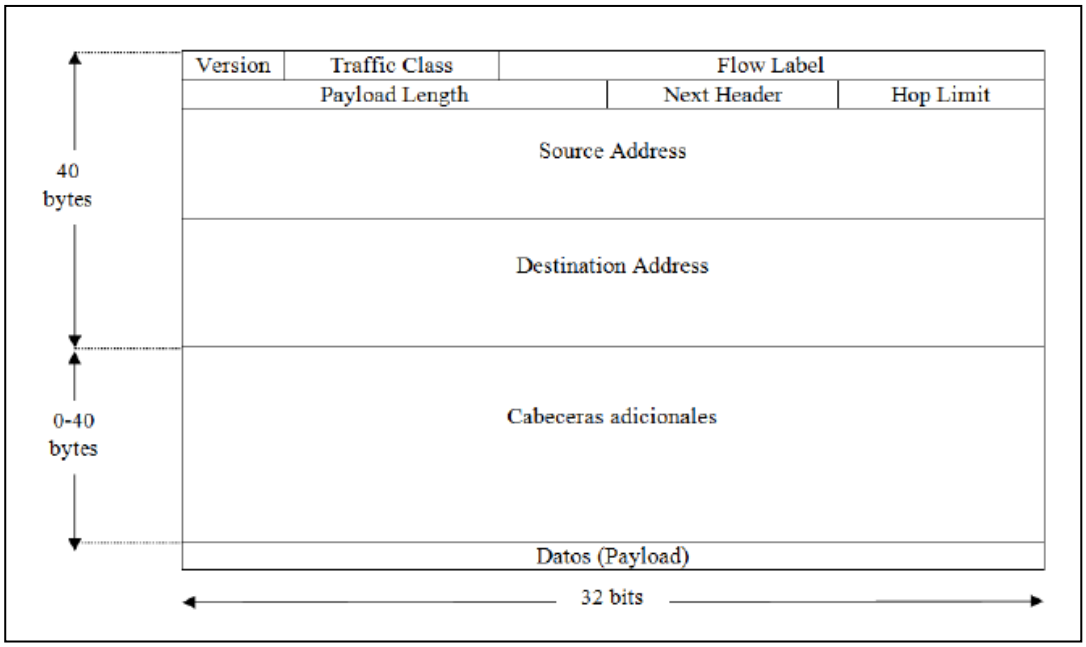



**FIGURA 2.4. ESTRUCTURA DE UN PAQUETE IPV6** [8]

## 2.4.2 DESCRIPCIÓN DE LA CABECERA EN IPv6

[8] **Fuente:** JARA Felipe; ESTUDIO E IMPLEMENTACIÓN DE UNA RED IPV6 EN LA UTFSM; Chile 2009. http://www.implementaciónIpv6_UTFSM_proyecto.pdf pág 14

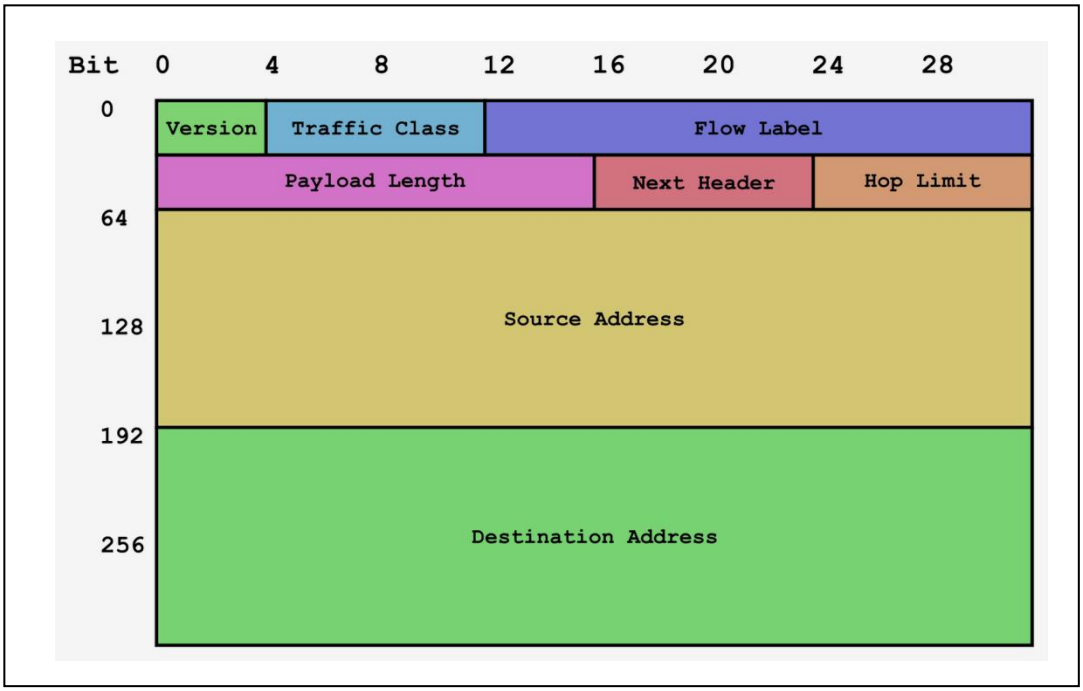



**FIGURA 2.5. CABECERA IPV6** [9]

| CAMPO | TAMAÑO | DESCRIPCIÓN |
|---|---|---|
| **Version** | 4 bits | «0110» indica versión 6. |
| **Traffic Class** | 8 bits | Se usa para identificar la «clase» de tráfico, o la prioridad, de forma que los paquetes se puedan reenviar con distintas prioridades para asegurar la QoS. Se utiliza para distinguir las fuentes que deben beneficiarse del control de flujo de otras. Se asignan prioridades de 0 a 7 a fuentes que pueden disminuir su velocidad en caso de congestión. Se asignan |

[9] **Fuente:** FERNANDEZ Azael; Tutorial IPv6; México 2010. http://www.tutorial-IPv6-UNAM.pdf. Pág 21

| | | |
|---|---|---|
| | | valores de 8 a 15 al tráfico en tiempo real (datos de audio y video incluidos) en donde la velocidad es constante. |
| **Flow Label** | 30 bits | Los paquetes que pertenecen a un flujo de clase de tráfico concreto se etiquetan para identificar a qué «flujo» pertenecen contiene un número único escogido por la fuente que intenta facilitar el trabajo de los routers y permitir la implementación de funciones de calidad de servicio como RSVP (Resource Reservation Setup Protocol [Protocolo de reserva de recursos]). Este indicador puede considerarse como un marcador de un contexto en el router. El router puede entonces llevar a cabo procesamientos particulares: escoger una ruta, procesar información en "tiempo real", etc. |
| **Payload Length** | 16 bits | Tamaño, en bytes, del resto del paquete, incluyendo las cabeceras de extensión. |
| **Next Header** | 8 bits | Identifica el tipo de cabecera que sigue inmediatamente a la cabecera de IPv6. Usa los mismos valores que en el campo Protocolo de IPv4 (RFC 1700). Puede ser un protocolo (de una capa superior ICMP, UDS, TCP, etc.) o una extensión. |

| | | |
|---|---|---|
| **Hop Limit** | 8 bits | Número de enlaces que puede atravesar un paquete antes de descartarlo. Cada vez que se reenvía este campo se decrementa en 1. Reemplaza el campo "TTL" (Time-to-Live [Tiempo de vida]) en IPv4, su valor disminuye con cada nodo que reenvía el paquete. Si este valor llega a 0 cuando el paquete IPv6 pasa por un router, se rechazará y se enviará un mensaje de error ICMPv6. Esto se utiliza para evitar que los datagramas circulen indefinidamente. Tiene la misma función que el campo Time to live (Tiempo de vida) en IPv4, es decir, contiene un valor que representa la cantidad de saltos y que disminuye con cada paso por un router. En teoría, en IPv4, hay una noción del tiempo en segundos, pero ningún router la utiliza. Por lo tanto, se ha cambiado el nombre para que refleje su verdadero uso. |
| **Source Address** | 128 bits | Dirección del nodo emisor |
| **Destination Address** | 128 bits | Dirección del nodo de destino, que puede ser un nodo final o un nodo intermedio. |

**Tabla III Descripción de la Cabeza IPv6**

### 2.4.3 Representación de las direcciones[10]

Existen tres formas de representar las direcciones IPv6 como cadenas de texto.

- x:x:x:x:x:x:x:x cada x representa el valor hexadecimal de los 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir uno número en cada campo.

Ejemplo:

| |
|---|
| DCFE:BA98:7654:3210:DCFE:BA98:7654:3210<br>2080:0:0:0:8:800:200C: 417ª |

- Como será común utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar constantemente :: para representarlos. El uso de :: indica uno o más grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección.

Ejemplo:

| | |
|---|---|
| 1080:0:0:0:8:800:200C:417A | Unicast address |
| FF01:0:0:0:0:0:0:101 | Multicast address |
| 0:0:0:0:0:0:0:1 | Loopbak address |
| 0:0:0:0:0:0:0:0 | Unspecified address |

Representación de la dirección IPv6

[10] Fuente: NOGUÉS Albert; Direccionamiento IPv4; 2008. http://www.albertnogues.com/attachments/014_IntroIp.pdf. pág 23

| | |
|---|---|
| 1080:0:0:0:8:800:200C:417A | Unicast address |
| FF01::101 | Multicast address |
| ::1 | Loopbak address |
| :: | Unspecified address |

Representación de la dirección IPv6 simplificada[11]

- Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis: x:x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4.

Ejemplos:

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

O de la forma simplificada

::13.1.68.3
::FFFF:129.144.52.38

[11] Fuente: JARA Felipe; ESTUDIO E IMPLEMENTACIÓN DE UNA RED IPV6 EN LA UTFSM; Chile 2009. http://www.implementacionipv6.utfsm. Pág 17

### 2.4.4 DIRECCIONAMIENTO

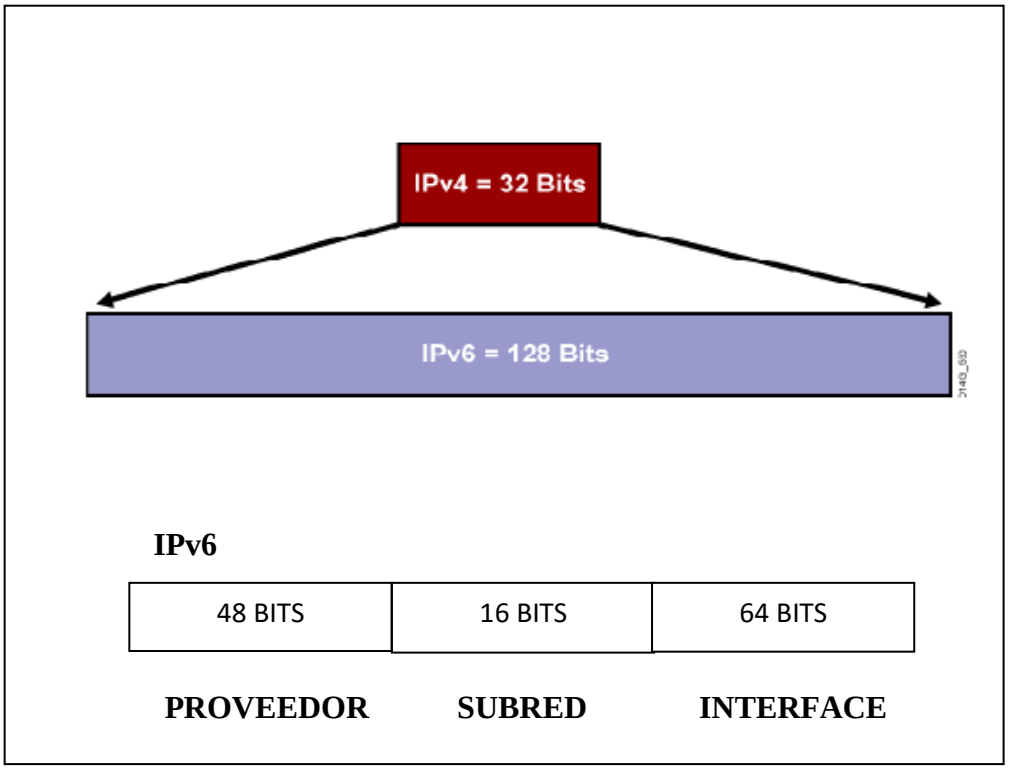



**FIGURA 2.6 DIRECCIONAMIENTO IPV6**

Las direcciones IPv6 son de 128 bits e identifican interfaces individuales o conjuntos de interfaces. Al igual que en Ipv4 en nodos se asignan a interfaces, y son de 32 bits.

#### 2.4.4.1 Guía de Direccionamiento IPv6

Para el direccionamiento en IPv6 se hablará en dos términos; parte de red y parte de interface (o llamado en IPv4, la parte del host), la interface para nosotros será los últimos 64 bits es decir, las subredes más pequeñas serán de 64 bits y los primeros 64 representarán la red, es decir, los 128 bits totales de cada dirección.

En IPv6 tenemos del bit 48 al 63 para segmentar, es decir con estos bits podemos tener 2^16 subredes, lo cual es más que suficiente para una Universidad, aquí indicamos una manera que será fácil de administrar. Gráficamente tenemos:

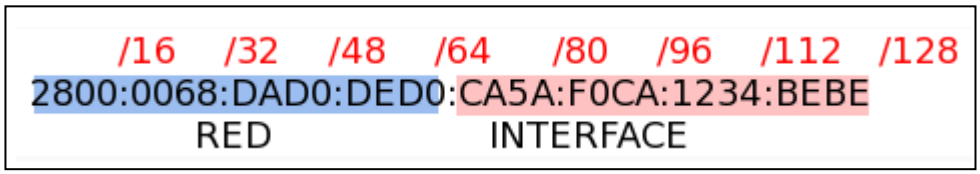



**FIGURA 2.7 REPRESENTACIÓN DE LA RED E INTERFACE[12]**

- Los primeros 32 bits ( 8 hexadecimales ) definen la red de CEDIA -> 2800:68[13]

- Los siguientes 16 bits (4 hexadecimales ) definen la red de la Universidad -> :DAD0:

- Los siguientes 16 bits (4 hexadecimales) definen a cada una de las redes de la Universidad :DED0:

- Los últimos 64 bits (16 hexadecimales) son los que definen a un host especifico: CA5A:F0CA:1234:BEBE.

### 2.4.4.2 TIPOS DE DIRECCIONAMIENTO IPv6[14]

Se clasifican en tres:

[12] Fuente: CHACON Claudio; Reto IPv6; Ecuador 2019. http://www.cedia.gob.ec
[13] Fuente: CHACON Claudio; Reto IPv6; Ecuador 2019. http://www.cedia.gob.ec
[14] Fuente: JARA Felipe; ESTUDIO E IMPLEMENTACIÓN DE UNA RED IPV6 EN LA UTFSM; Chile 2009. http://www.implementacionipv6.utfsm. Págs. 17-22

- Unicast identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado solo a la interfaz identificada con dicha dirección.

- Anycast identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto a la cual pertenece esa dirección anycast.

- Multicast identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todas las interfaces del grupo identificadas con esa dirección.

    - En Ipv6 no existen direcciones broadcast, ya que su funcionalidad ha sido mejorada por las direcciones multicast que identifican a determinados grupos de dispositivos en una red.

#### 2.4.4.2.1 Unicast

Las direcciones “unicast” cumplen la función de individualizar a cada nodo conectado a una red. Esto permite otorgar conectividad punto a punto entre los nodos pertenecientes a ella.

Uno de los nuevos aspectos introducidos en IPv6 es el uso de contextos en las direcciones “unicast”. Los contextos definen el dominio de una red, ya sea lógico o físico. El poder reconocer el contexto al que pertenece una determinada dirección permite realizar un manejo óptimo de los recursos de la red, optimizando su desempeño. En IPv6, las direcciones unicast pueden pertenecer a uno de los tres contextos existentes:

- Local al enlace (“link-local”): Identifica a todos los nodos dentro de un enlace (capa 2).

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

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

### 2.4.4.2.1.1 Direcciones Link-Local

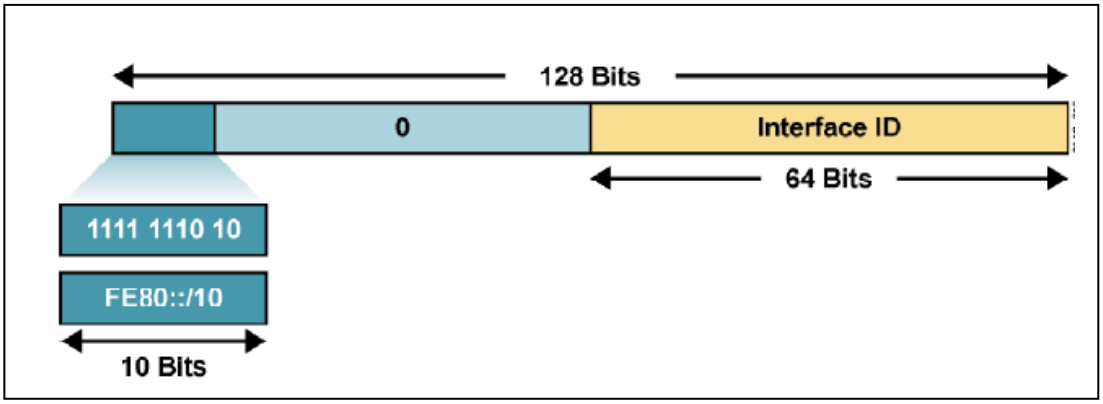



**FIGURA 2.8 DIRECCIÒN LINK LOCAL** [15]

- Son creadas dinámicamente en todas las interfaces IPv6 utilizando el prefijo FE80::/10 identificador de interfaz. El identificador de interfaz se genera automáticamente a partir de su dirección MAC, siguiendo el formato EUI-64.

- Se utiliza para la configuración automática de direcciones, descubrimiento de vecinos y descubrimiento de Gateway.

- Conectan dispositivos en la misma red local sin necesidad de direcciones globales, similar a las direcciones privadas en IPv4.

[15] Fuente: OSTLING Janne; ipv6 for dummies; USA 2008. http://www. ipv6-for-dummies-se-090120.pdf. pág. 23

- Para la comunicación entre nodos se debe especificar la interface de salida, ya que todas las interfaces están conectadas a FE80::/10.

**NOTA:**

- El Institute of Electrical and Electronic Engineers (IEEE) define la dirección EUI-64 de 64 bits. Las direcciones EUI-64 se asignan a un adaptador de red o se derivan de las direcciones IEEE 802.

- **Direcciones IEEE 802**

  Los identificadores de interfaz tradicionales para los adaptadores de red utilizan una dirección de 48 bits que se llama dirección IEEE 802. Esta dirección consta de un Id. de compañía (también llamado Id. de fabricante) de 24 bits y un Id. de extensión (también llamado Id. de tarjeta) de 24 bits. La combinación del Id. de compañía, que se asigna de forma única a cada fabricante de adaptadores de red, y el Id. de tarjeta, que se asigna de forma única a cada adaptador de red en el momento del ensamblaje, genera una dirección única global de 48 bits. Esta dirección de 48 bits también se denomina dirección física, de hardware o de control de acceso a medios (MAC, Media Access Control).

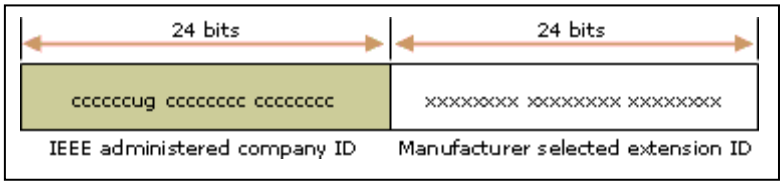



**FIGURA 2.9 IEEE 802** [16]

[16] **Fuente:** CORONADO Moisés; DISEÑO E IMPLEMENTACIÓN DE SOFTWARE PARA PROTOCOLO IPV6; Chile 2004.
http://www.cybertesis.uach.cl/tesis/uach/2004/bmfcic822d/doc/bmfcic822d.pdf. pág. 39

### 2.4.4.2.1.2 Direcciones “unicast” locales únicas

- Las direcciones locales únicas son direcciones que permiten la comunicación de nodos al interior de un sitio.

- Se entiende por sitio a toda red organizacional, de prefijo /48, compuesta por 1 o más subredes.
- Son el equivalente a las direcciones privadas en IPv4, cumpliendo la misma función: proveer conectividad entre los nodos de un sitio ó “intranet”.

- Al igual que las direcciones locales al enlace, no pueden ser enrutadas hacia Internet. Su estructura se detalla en la Figura.

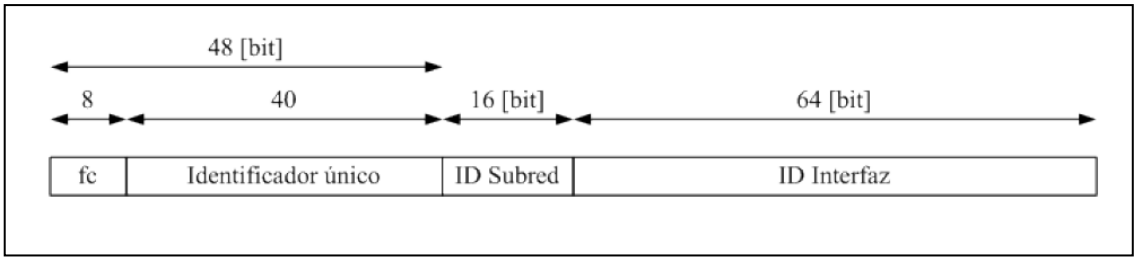



**FIGURA 2.10 ESTRUCTURA DE UNA DIRECCIÓN LOCAL ÚNICA.**[17]

Todas las direcciones locales únicas se encuentran dentro del rango dado por el prefijo fc00::/8. Los campos de una dirección “unicast” local única son:

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

[17] **Fuente:** JARA Felipe; ESTUDIO E IMPLEMENTACIÓN DE UNA RED IPV6 EN LA UTFSM; Chile 2009. http://www.implementacionipv6.utfsm. Pág. 20

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

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

### 2.4.4.2.1.3 Direcciones "unicast" Globales:

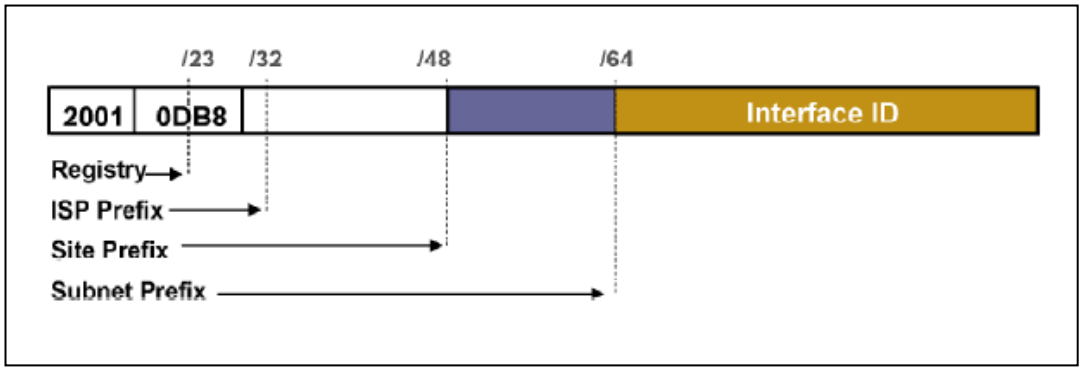



**FIGURA 2.11 DIRECCIÓN UNICAST GLOBAL Y ANYCAST**[18]

- Las direcciones unicast globales son usadas para comunicar 2 nodos a través de Internet.

- Son el único tipo de direcciones que pueden ser enrutadas a través del internet.

- Utiliza un prefijo de enrutamiento global. Facilita la agregación.

- Una interface puede tener varias direcciones: unicast, anycast, multicast.

[18] Fuente: OSTLING Janne; ipv6 for dummies; USA 2008. http://www.ipv6-for-dummies-se-090120.pdf. Pág. 24

- Eventualmente cada interface puede tener múltiples direcciones locales y globales únicas.

### 2.4.5 MECANISMOS DE CONFIGURACIÓN DE DIRECCIONES

En IPv6 existen tres distintas formas en las que un nodo puede obtener una dirección

IPv6: de forma estática, autoconfiguración sin estados y mediante DHCPv6.

#### 2.4.5.1 Configuración estática

La configuración estática consiste en ingresar manualmente la dirección IPv6 de un nodo en un archivo de configuración o mediante el uso de herramientas propias del sistema operativo. La información que se debe incluir como mínimo es la dirección IPv6 y el tamaño del prefijo de red.

#### 2.4.5.2 Autoconfiguración sin estados (“stateless”)

El procedimiento de autoconfiguración sin estados utiliza el protocolo de descubrimiento de vecinos NDP para reconocer a los “routers” presentes en el enlace y generar una dirección IPv6 a partir del prefijo que estos anuncias. Los pasos que realiza un nodo para obtener una dirección son los siguientes:

- Descubrir un prefijo utilizado en el enlace: El nodo escucha los anuncios que envían los “routers” periódicamente enviando un mensaje de solicitación de “router”.

- Generar un identificador de interfaz: Para generar el resto de la direcciónIPv6, el nodo genera un identificador de interfaz. Puede generarla a partir de su dirección MAC (como en las direcciones locales al enlace) o de forma aleatoria.

- Verificar que la dirección no esté duplicada: La dirección IPv6 generada debe ser única, por lo que el nodo inicia el procedimiento de detección de direcciones duplicadas (DAD). Si la dirección es única, el nodo comienza a utilizarla.

### 2.4.5.3 Autoconfiguración con estados (DHCPv6)

La implementación de DHCP para IPv6 (DHCPv6) realiza las mismas funciones que DHCP en IPv4. Un servidor DHCP envía mensajes que contienen la dirección IPv6 a utilizar, dirección del servidor DNS e información adicional a los clientes DHCP, quienes se configuran de acuerdo a la información recibida.

A diferencia de la configuración sin estados, el uso de DHCPv6 permite centralizar toda la asignación de direcciones de los equipo pertenecientes a un sitio. El servidor DHCPv6 no necesita estar conectado en el mismo enlace de los clientes DHCPv6, los mensajes pueden ser enrutados.

**NOTA:**

- En el protocolo IPv6 DHCP ya no es necesario por lo que las direcciones IP podrán ser obtenidas de forma totalmente automática, lo que facilitará enormemente la creación de redes, tanto a nivel local como a nivel extremo.

### 2.4.6 PROTOCOLO ENRUTADO.

Es cualquier protocolo de red que ofrezca información en su dirección de capa de red para que permita que un paquete sea enviado desde un host a otro. Un protocolo enrutado utiliza las tablas de enrutamiento para enviar los paquetes[19].

### 2.4.7 PROTOCOLO DE ENRUTAMIENTO[20]

Los protocolos de enrutamiento permiten enrutar los protocolos enrutados, es decir, suministran los mecanismos necesarios para compartir la información de enrutamiento.

Los protocolos de enrutamiento dejan que los routers puedan comunicarse entre ellos, permitiendo dirigir o enrutar los paquetes, es decir, determina el camino más corto para hacer llegar el mensaje.

Los Routers conocen las rutas disponibles por medio del enrutamiento estático o dinámico.

#### 2.4.7.1 Enrutamiento Estático

El conocimiento de las rutas estáticas es gestionado manualmente por el administrador de la red. El administrador debe actualizar manualmente cada entrada de ruta estática siempre que un cambio en la topología requiera una actualización.

#### 2.4.7.2 Enrutamiento dinámico

[19] Fuente: CLEVELAND Chris ACADEMIA DE NETWORKING DE CISCO SYSTEMS, Cisco "Guía del Primer Ano CCNA 1 y 2", Tercera Edición, Editorial Pearson Educacion, S.A. Madrid, 2004. Pág. 626

[20] Fuente: CARRILLO Vilma; Protocolos de Enrutamiento; Colombia 2010. http://www.Slideshare.net/ VILMACARRILLO/protocolos-de-enrutamiento-5139157

El enrutamiento dinámico se utiliza cuando alguna de las condiciones del enrutamiento estático no se cumple. Una ruta dinámica es construida por información intercambiada por los protocolos de enrutamiento. Los protocolos son diseñados para distribuir información que dinámicamente ajustan las rutas reflejadas en las condiciones de la red. Los protocolos de enrutamiento manejan complejas situaciones de enrutamiento más rápido de lo que un administrador del sistema podría hacerlo. Una red con múltiples caminos a un mismo destino puede utilizar enrutamiento dinámico.

### 2.4.7.3 Análisis entre el enrutamiento dinámico y estático.

| Enrutamiento Dinámico | | Enrutamiento Estático |
|---|---|---|
| **Complejidad de la configuración** | Es independiente del tamaño de la red | Se incrementa con el tamaño de la red |
| **Conocimientos requeridos del administrador** | Se requiere de un conocimiento avanzado | No se requiere de conocimientos adicionales |
| **Cambios de Topología** | Se adapta automáticamente a los cambios de topología | Requiere la intervención del administrador |
| **Escalamiento** | Adecuado para topologías simples y complejas | Adecuada para topologías simples |
| **Seguridad** | Es menos segura | Es más segura |
| **Uso de recursos** | Utiliza memoria y ancho de banda del enlace | No necesita recursos adicionales |
| **Capacidad de predicción** | La ruta depende de la topología actual | La ruta hacia el destino es siempre la misma |

**Tabla IV ENRUTAMIENTO DINÁMICO VS ESTÁTICO[21]**

[21] Fuente: ULLOA Julio; Implementación de protocolos de enrutamiento mediante un enrutador basado en software de código abierto bajo Linux; Ecuador 2007. http://www. bibdigital. epn. edu. ec/ bitstream/15000/544/1/CD-1048.pdf. pág. 28

## 2.5 LA TRANSICIÓN A IPV6 ES UNA NECESIDAD

Dado que el protocolo predominante en la actualidad en Internet es IPv4, e Internet se ha convertido en algo vital, no es posible su sustitución, es decir, no es posible apagar la Red, ni siquiera por unos minutos y cambiar a IPv6. Sin embargo, IPv6 se está implementando lentamente y en redes selectas. Debido a las mejores herramientas, tecnologías y administración de direcciones en los últimos años, Lo que permitirá a IPv6 podrá reemplazar a IPv4 como protocolo de Internet dominante.

Precisamente por ello, la organización encargada de la estandarización de los protocolos de Internet (IETF, Internet Engineering Task Force), diseñó junto con el propio IPv6, una serie de mecanismos que llamamos de transición y coexistencia.

Básicamente es importante entender lo que ello implica. No se trata de una migración como erróneamente se indica en muchas ocasiones, sino que ambos protocolos, IPv4 e IPv6, existirán durante algún tiempo, es decir se produce una coexistencia. Cabe recalcar que IPv4 no desaparecerá de la noche a la mañana. En realidad, coexistirá durante un tiempo con IPv6 y será reemplazado gradualmente por éste.

Por lo que se utilizarán mecanismos de transición que son un conjunto de mecanismos y de protocolos implementados en hosts y routers, junto con algunas guías operativas de direccionamiento designadas para hacer la transición de Internet al IPv6 con la menor interrupción posible. Para ello hay tres posibles soluciones técnicas: dual stack, tunnelling y translators.

### 2.5.1 Método de transición Dual Stack

La técnica “dual stack” es aquella en donde se ejecutan los protocolos IPv4 e IPv6 de manera simultánea en los nodos de una red. Cada nodo tiene asignada direcciones IPv4 e IPv6. Esta técnica tiene la ventaja de asegurar la conectividad de los nodos de la red, cuando no sea posible utilizar IPv6, se puede utilizar IPv4.

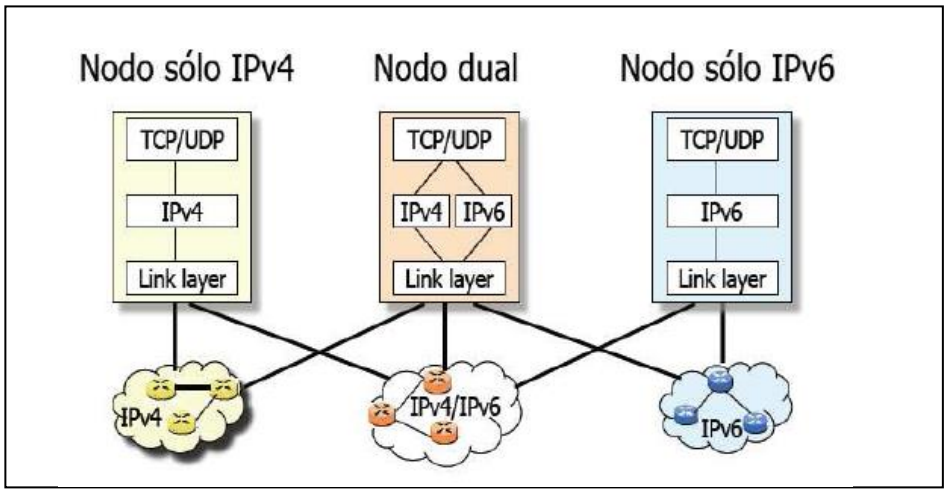



**FIGURA 2.12 MÉTODO DE TRANSICIÓN DUAL STACK** [22]

Es una de las técnicas más utilizadas, ya que puede ser utilizada en las diferentes partes de la red: equipos clientes, servidores y routers. Para que trabaje eficazmente, el dual stack debe ser implementado en todos los routers de la red. No habrá comunicación entre IPv4 e IPv6; sino que las aplicaciones tendrán que soportar ambos modos. El reto con dual stack es que todos los equipos de la red deben contar con la suficiente potencia de proceso y memoria, para gestionar dos pilas IP diferentes.

[22] Fuente: AHUATZIN Gerardo; Desarrollo de un esquema de traducción de direcciones IPv6-IPv4-IPv6; http://www.catarina.udlap.mx/u_dl_a/tales/documentos/lis/...s.../capitulo2.pdf. pág. 64

### 2.5.2 Método de transición Tunneling

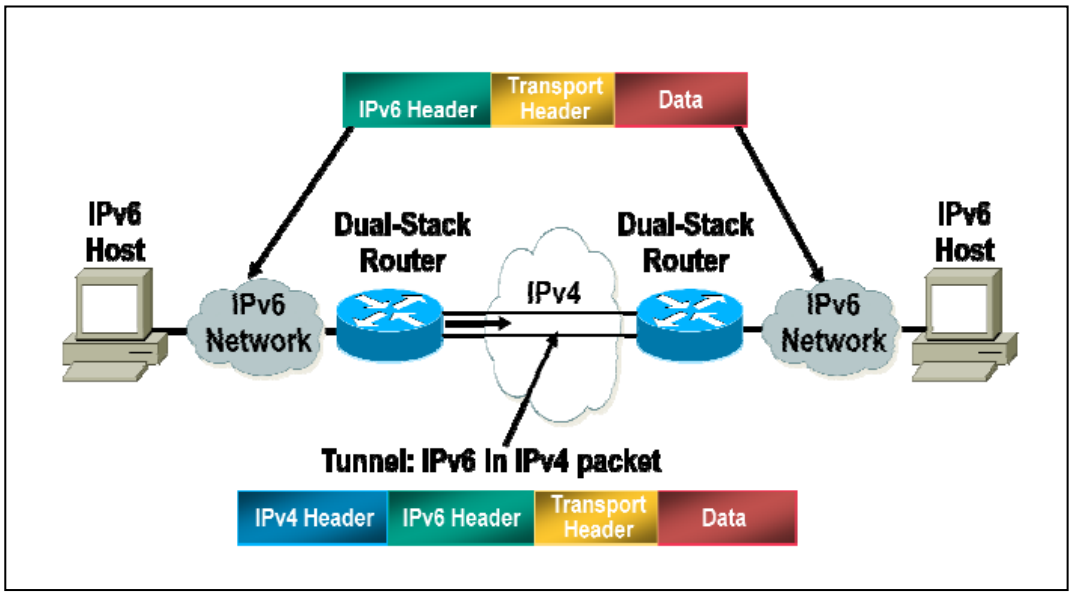



**FIGURA 2.13 MÉTODO DE TRANSICIÓN TUNNELING[23]**

Cuando un paquete IPv6 tiene que atravesar una red que sólo es IPv4, pueden utilizarse "túneles" para lograrlo. El tunneling es un método de integración en el que un paquete IPv6 se encapsula dentro de otro protocolo como lo es IPv4. Este mecanismo permite la conexión entre redes IPv6 sin la necesidad de convertir las redes intermedias a IPv6. Cuando se utiliza IPv4 para encapsular el paquete IPv6, se especifica el tipo de protocolo en el encabezado de IPv4 y el paquete incluye un encabezado de IPv4 de 20 bytes sin opciones y un encabezado y contenido de IPv6. El paquete es "desencapsulado" al llegar al destino, que deberá ser un nodo IPv6 o dual stack. El uso de túneles requiere que exista un equipo en cada extremo que realice el proceso de encapsulación y extracción de los paquetes IPv6. También requiere routers de stack doble.

[23] Fuente: OSTLING Janne; ipv6 for dummies; USA 2008. http://www. ipv6-for-dummies-se-090120.pdf. pág. 78

### 2.5.3 Método de transición Translators NAT-PT (Network Address Translation – Protocol Translation)

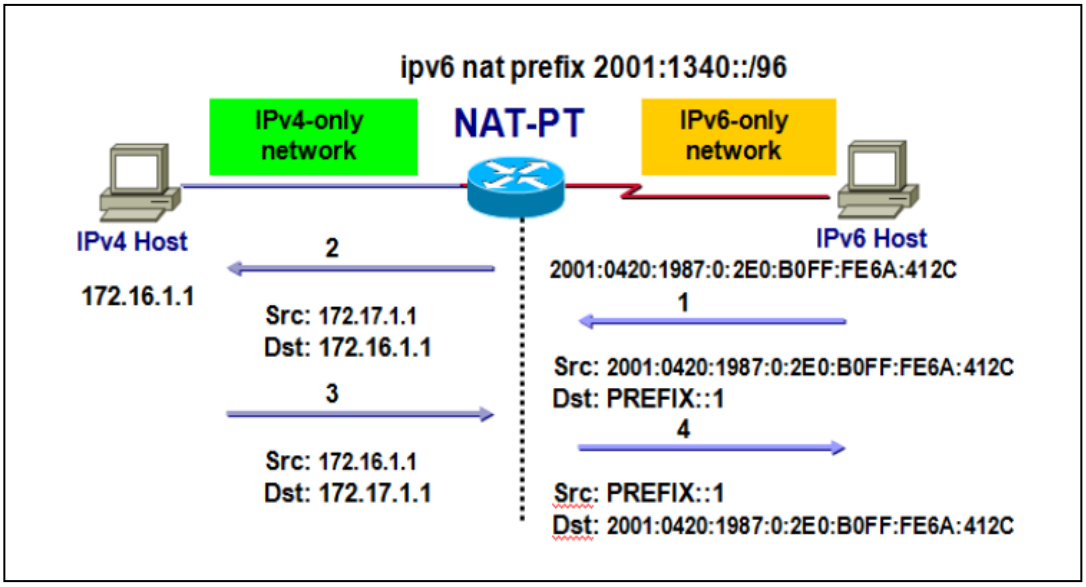



**FIGURA 2.14 MÉTODO DE TRANSICIÓN TRANSLATORS**[24]

Este mecanismo de transición realiza una "traducción" similar a la que efectúa el NAT, donde es modificada la cabecera IPv4 a una cabecera IPv6. El más conocido dentro de este grupo es NAT-PT. Sin embargo, este tipo de mecanismos no es de los más recomendados.

## 2.6 IMPLEMENTACIÓN DOBLE-PILA

Este enfoque de doble pila es un mecanismo fundamental para introducir IPv6 en las arquitecturas IPv4 actuales y se prevé que siga siendo muy utilizado durante el próximo futuro. Su punto flaco es que obliga a que cada máquina retenga una dirección IPv4, cada vez más escasas. Así, a medida que se difunde IPv6, la técnica de doble pila tendrá que ser aplicada allí donde específicamente ayuda al

[24] Fuente: OSTLING Janne; ipv6 for dummies; USA 2008. http://www. ipv6-for-dummies-se-090120.pdf. pág. 101

proceso de transición, por ejemplo en routers y servidores. Un servidor de doble pila puede soportar clientes sólo IPv4 convencionales, nuevos clientes sólo IPv6, y por supuesto clientes de doble pila. Para aquellos casos en que haya insuficientes direcciones IPv4 se ha definido una combinación del modelo de conversión y de doble pila de protocolos, conocido como DSTM (Dual Stack Transition Mechanism).

### 2.6.1 El modelo de referencia OSI

El modelo OSI está constituido por 7 capas que definen las funciones de los protocolos de comunicaciones. Cada capa del modelo representa una función realizada cuando los datos son transferidos entre aplicaciones cooperativas a través de una red intermedia.

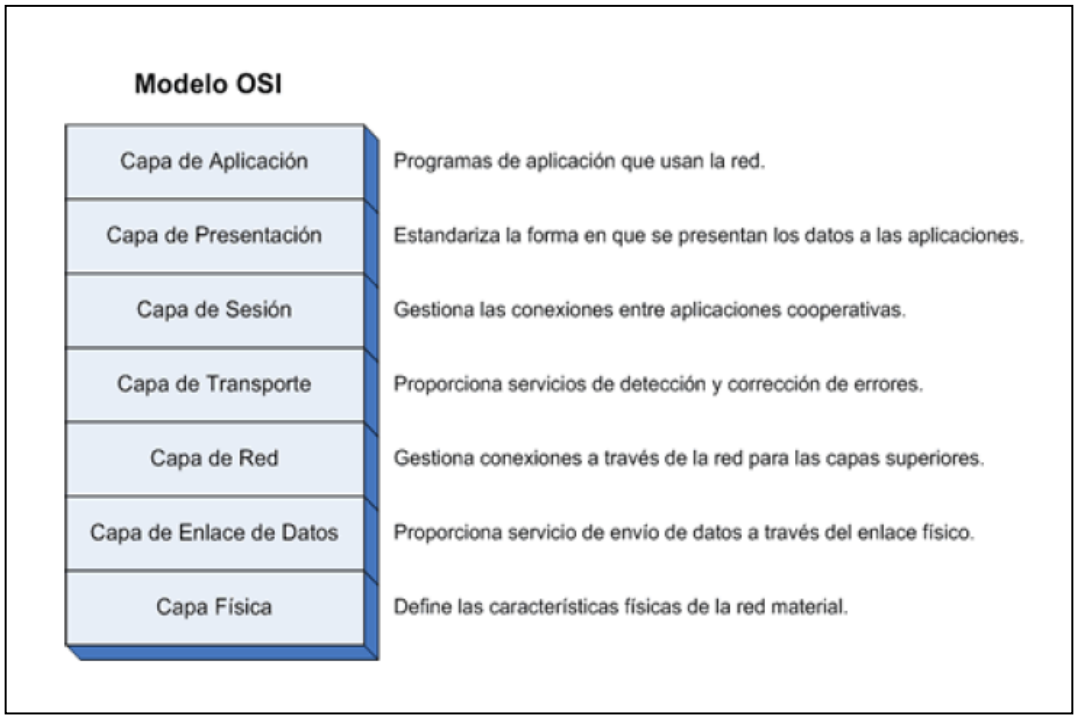



**FIGURA 2.15 MODELO OSI**[25]

[25] Fuente: OSTLING Janne; ipv6 for dummies; USA 2008. http://www. ipv6-for-dummies-se-090120.pdf. pág. 33

### 2.6.2 Capas o niveles del TCP/IP

Para conseguir un intercambio fiable de datos entre dos computadoras, se deben llevar a cabo muchos procedimientos separados.

El resultado es que el software de comunicaciones es complejo. Con un modelo en capas o niveles resulta más sencillo agrupar funciones relacionadas e implementar el software de comunicaciones modular.

Las capas están jerarquizadas. Cada capa se construye sobre su predecesora. El número de capas y, en cada una de ellas, sus servicios y funciones son variables con cada tipo de red. Sin embargo, en cualquier red, la misión de cada capa es proveer servicios a las capas superiores haciéndoles transparentes el modo en que esos servicios se llevan a cabo. De esta manera, cada capa debe ocuparse exclusivamente de su nivel inmediatamente inferior, a quien solicita servicios, y del nivel inmediatamente superior, a quien devuelve resultados.

### 2.6.3 Capas del modelo TCP/IP

**Capa 4:** Aplicación, se diseñó como una capa protocolar que incluía detalles de las capas de sesión, presentación y aplicación del modelo OSI. La capa de aplicación manipula protocolos de alto nivel y temas de presentación, codificación y control del dialogo.

**Capa 3:** Transporte, similar a la capa 4 (transporte) del modelo OSI. La capa de transporte proporciona servicios de transporte desde un host de origen a un host de destino.

**Capa 2:** Internet, similar a la capa 3 (red) del modelo OSI. La función de la capa de internet es transportar los paquetes entre los hosts tratando de colocar la menor carga posible en la red. La Capa 3 no se ocupa de ni advierte el tipo de

comunicación contenida dentro de un paquete. Esta responsabilidad es la función de las capas superiores a medida que se requieren.

**Capa 1:** Acceso a Red, similar a la capa 1 (física) y 2 (enlace de datos) del modelo OSI. Capa de acceso a red es la que se ocupa de todos los temas que un paquete IP necesita para crear un enlace físico con el medio de red.

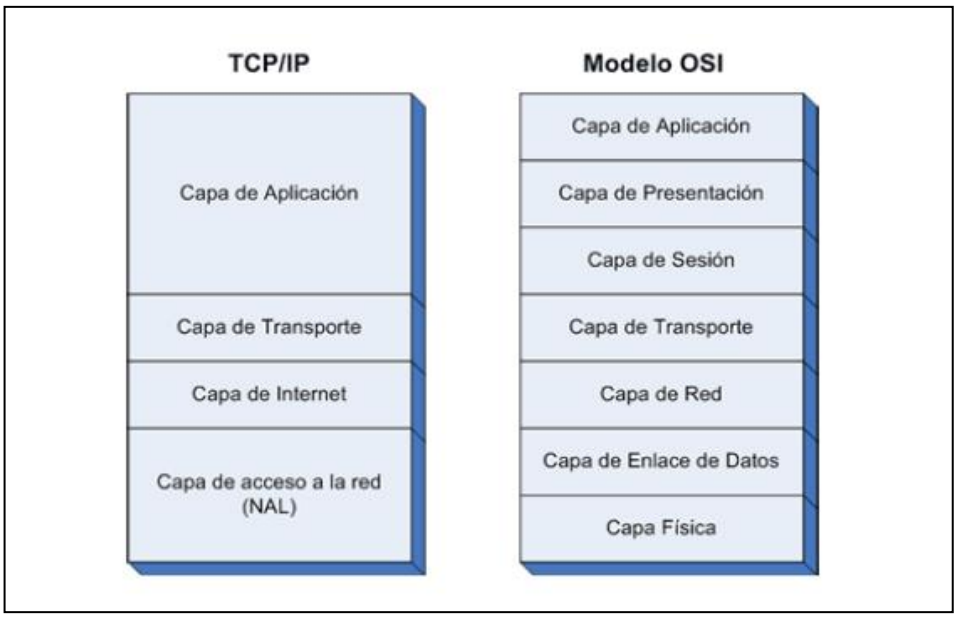



**FIGURA 2.16 COMPARACIÓN EN LOS MODELOS OSI Y TCP/IP[26]**

Es importante saber que algunas capas del modelo TCP/IP tienen los mismos nombres que ciertas capas del modelo OSI por lo que hay que tener en cuenta y no confundir las funciones de las capas de los dos modelos. Se observa en la Figura 2.16 que el número de capas es diferente, de modo que las funciones que lleva a cabo la capa dos en el modelo OSI no podrían ser las mismas que se realicen en la capa dos del modelo TCP/IP.

[26] Fuente: OSTLING Janne; ipv6 for dummies; USA 2008. http://www.ipv6-for-dummies-se-090120.pdf. Pág. 34

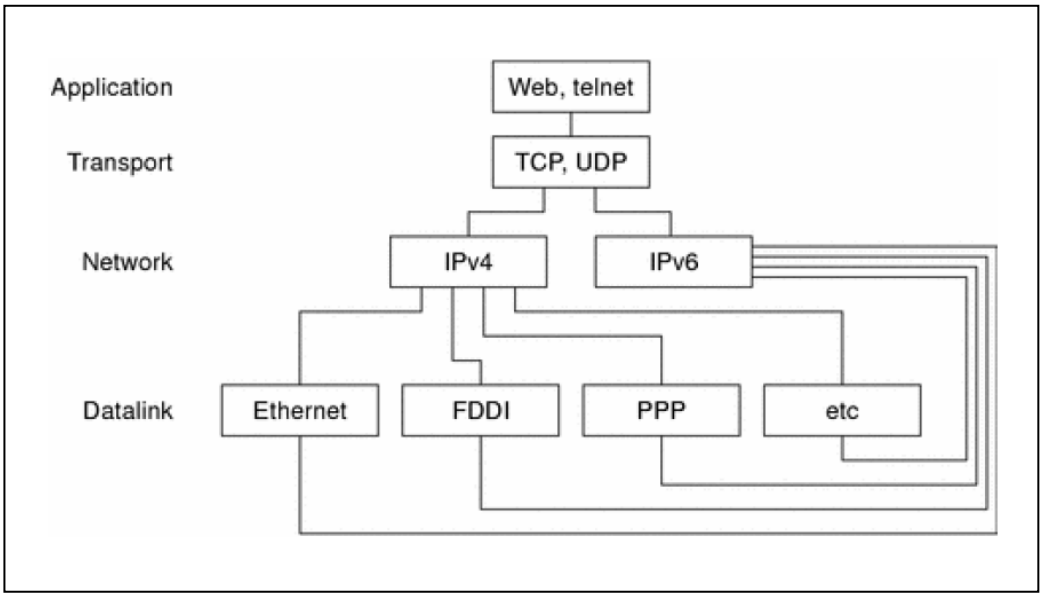



**FIGURA 2.17 DOBLE PILA EN EL MODELO OSI[27]**

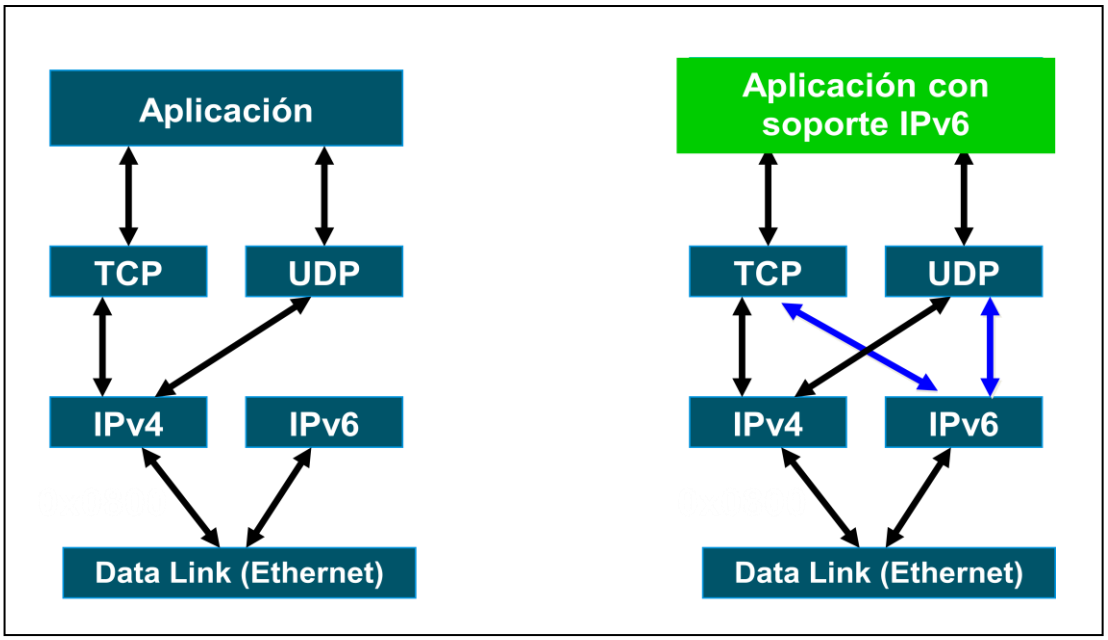



**FIGURA 2.18 DUAL STACK EN LOS SERVIDORES DE APLICACIONES[28]**

[27] Fuente: OSTLING Janne; ipv6 for dummies; USA 2008. http://www.ipv6-for-dummies-se-090120.pdf. Pág. 35

[28] Fuente: OSTLING Janne; ipv6 for dummies; USA 2008. http://www. ipv6-for-dummies-se-090120.pdf. Pág. 68

- Modo Dual stack significa:
  - Ambas pilas IPv4 and IPv6 habilitadas
  - Las aplicaciones se comunican por IPv4 y IPv6
  - Selección de la versión está basada en la resolución de nombres y la preferencia de la aplicación.

# CAPITULO III

## 3. ANALISIS DE LA RED INSTITUCIONAL.

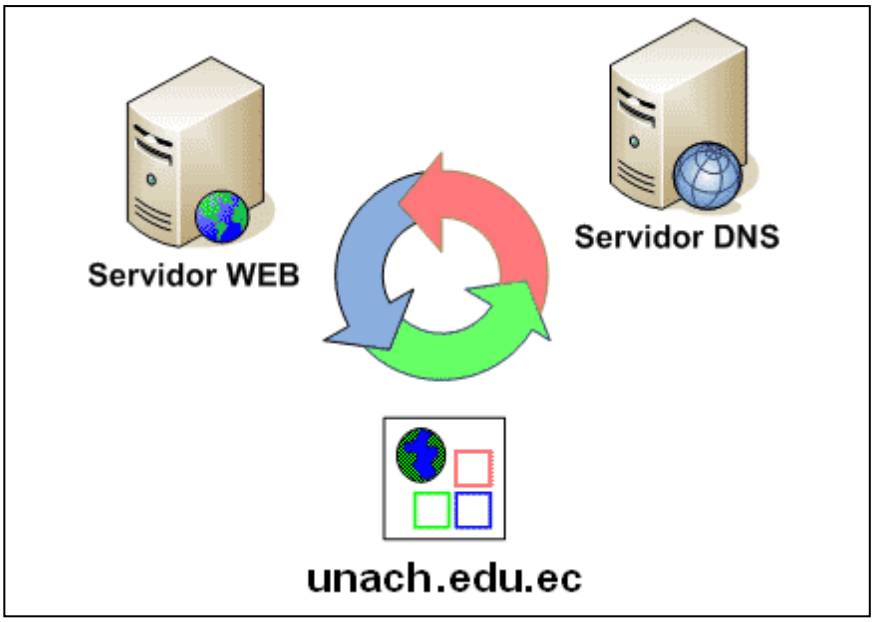



**FIGURA 3.1 SERVIDORES A IMPLEMENTAR**

### 3.1 INTRANET DE LA UNACH.

La Universidad Nacional de Chimborazo en su tecnología de red posee un backbone de fibra óptica, redes locales en cada una de sus Facultades, dispositivos de comunicación y personal técnico; recursos a través del cual se brinda servicios de acceso a internet, videoconferencia, biblioteca virtual los cuales apoyan a la gestión académica, administrativa, sistema financiero y recursos humanos de la institución.

Actualmente la UNACH está controlada por el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA), el mismo que contrata a la empresa TELCONET para que sea nuestro proveedor de internet. Los equipos activos de

red que permiten toda la interconexión local de comunicaciones de la UNACH se encuentran ubicados físicamente en la Facultad de Ingeniería (Centro de Cómputo y Sistemas).

Actualmente están conectadas al servicio de internet un promedio de 456 computadoras distribuidas en cada facultad (no se consideran conexiones inalámbricas) de la siguiente manera.

| **UNIDAD** | **PC'S** |
|---|---|
| Laboratorios Facultad de Ingeniería | 103 PC's |
| Laboratorios Facultad de Ciencias de la Salud | 44 PC's |
| Laboratorios Facultad de Ciencias Políticas | 37 PC's |
| Administrativo Facultad de Ingeniería | 40 PC's |
| Administrativo Facultad de Ciencias de la Salud | 22 PC's |
| Administrativo Facultad de Ciencias Políticas | 20 PC's |
| Edificio Administrativo | 130 PC's |
| Vicerrectorado Administrativo | 60 PC's |
| **TOTAL** | **456 PC's** |

**Tabla V Conexiones Internet Institucional**

El monitoreo de la red es centralizado, la seguridad se encuentra manejada a través de un firewall y redes de área virtual que permite ejercer control de acceso

proporcionando al administrador de la red información acerca del tipo y cantidad de trafico cursado a través del mismo.

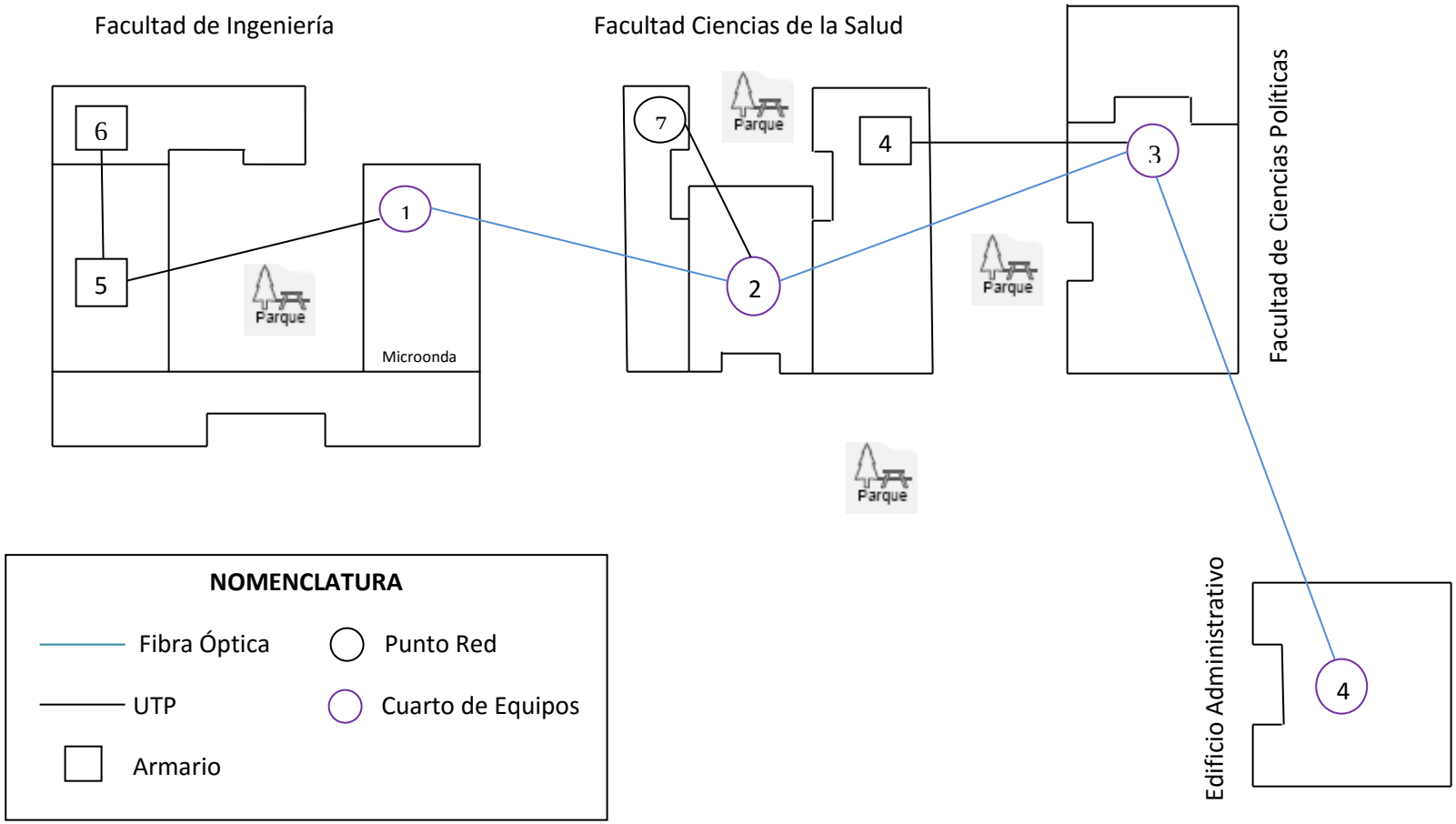



**Figura 3.2 BACKBONE CAMPUS EDISON RIERA**

| Numeración | Descripción | Ubicación | Funciones |
|---|---|---|---|
| 1 | Cuarto de equipos | Edificio Ingeniería, 3er. Piso, Oficinas Centro de Computo | Conexión a microonda del campus Dolorosa<br>Distribución de cableado en la Facultad de Ingeniería<br>Distribución de red hacia la Facultad de Ciencias de la Salud |
| 2 | Cuarto de equipos | Edificio Facultad de Ciencias de la Salud, 2do. Piso, Oficinas Centro de Computo | Conexión a Edificio Ciencias Políticas<br>Distribución de cableado en el Edificio de la Facultad de Ciencias de la Salud |
| 3 | Cuarto de equipos | Edificio Ciencias Políticas, Planta baja | Distribución de cableado en el Edificio y hacia el edificio administrativo |
| 4 | Cuarto de equipos | Edificio Administrativo, 3era Planta baja, cuarto de control | Distribución de cableado en el edificio administrativo |
| 5 | Armario de comunicaciones | Edificio Ingeniería, Bloque A, 2do. Piso, Oficinas | Acceso a la red |
| 6 | Armario de comunicaciones | Edificio Ingeniería, Bloque B, 1er. Piso, Biblioteca | Acceso a la red |
| 7 | Armario de comunicaciones | Edificio Ciencias de la Salud, 2 Piso. Auditorio | Acceso a la red |

**TABLA VI NOMENCLATURA BACKBONE CAMPUS EDISON RIERA**

## 3.2 MEDIOS DE TRANSMISIÓN DE LA INTRANET DE LA UNACH

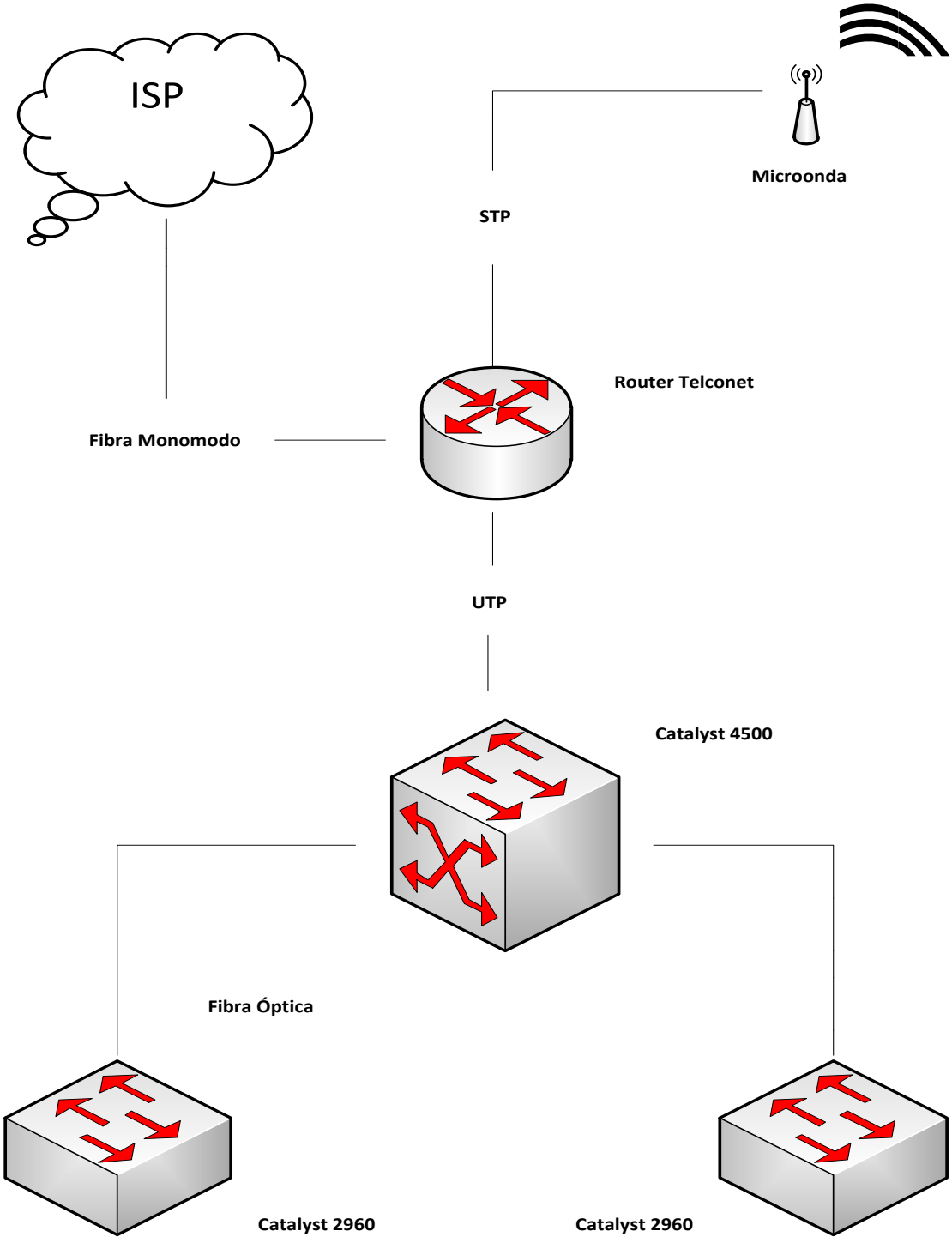



**FIGURA 3.3 TRANSMISION DE LA RED DE LA UNACH**

| Siglas | Descripción | Ubicación - Detalles |
|---|---|---|
| MDF | Armario Principal | Centro de Computo (Edificio Administrativo 3er. Piso) |
| IDF | Armario de Interconexión | Centro de Computo (Edificio Facultad de Ingeniería 3er. Piso) |
| IDF | Armario de Interconexión | Edificio Facultad de Ciencias de la Salud (1er, 2do, 4to. Piso) |
| IDF | Armario de Interconexión | Edificio Facultad de Ciencias Políticas (1er, 4to. Piso) |
| MCC | Cableado armario principal | Fibra Óptica, Cable UTP Cat. 5E, Cat. 6, uso de organizadores de cableado |
| ICC | Cableado armario interconexión | Fibra Óptica, Cable UTP Cat. 5E, Cat. 6, uso de organizadores de cableado |
| HCC | Cableado armario de planta | Cable UTP Cat. 5E, uso de organizadores de cableado |
| POP | Punto de presencia | En los edificios del campus |

**TABLA VII ELEMENTOS CABLEADO ESTRUCTURADO CAMPUS EDISON RIERA**

## 3.3 ESTRUCTURA LÓGICA DE LA INTRANET DE LA UNACH

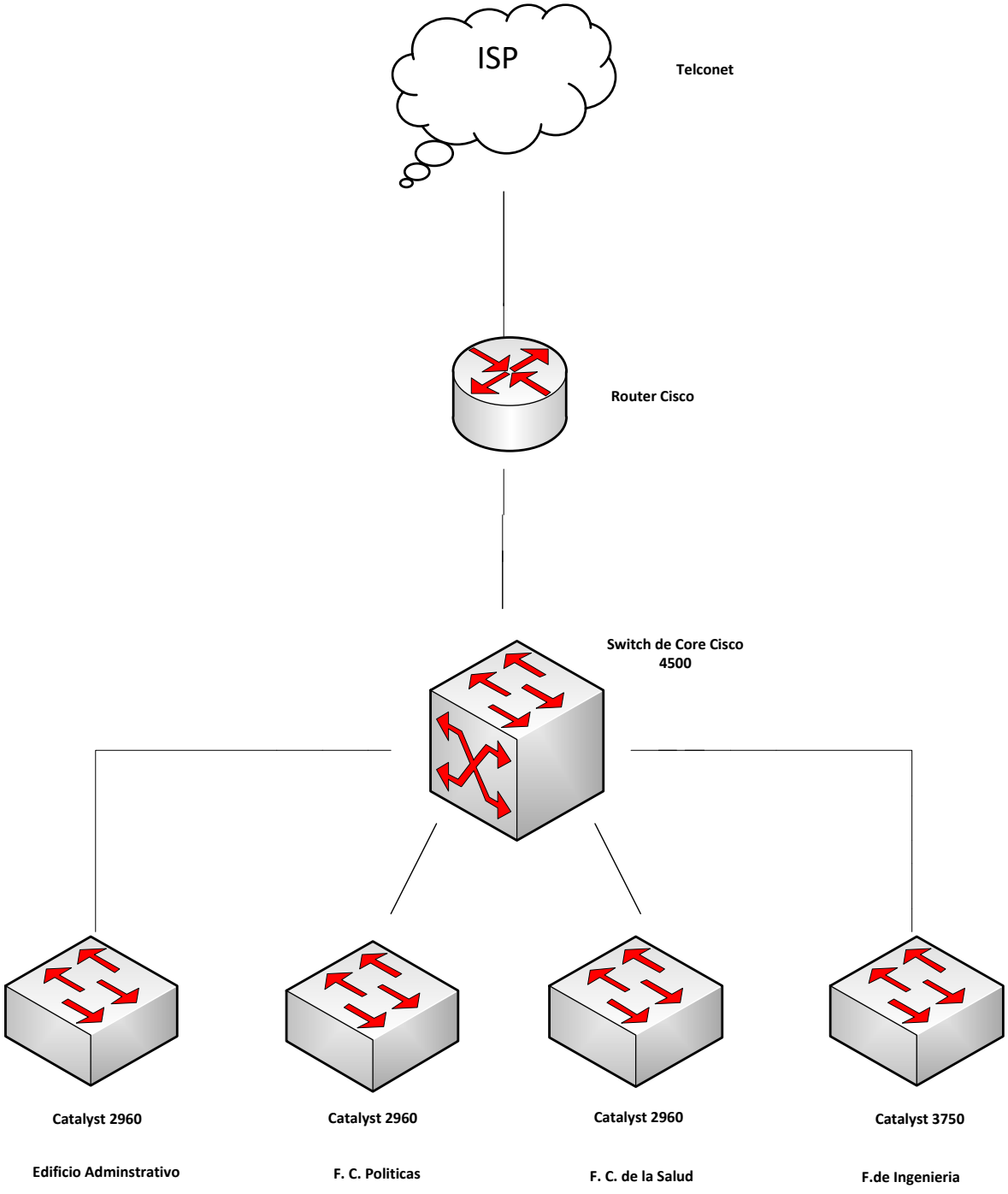



**FIGURA 3.4 ESTRUCTURA LOGICA INTRANET**

## 3.4 ANÁLISIS DEL SOPORTE IPV6 EN LA RED INSTITUCIONAL

El uso de la técnica “dual-stack” requiere que todos los equipos involucrados en conectar la red institucional a Internet cuenten con soporte para IPv6. En la **Tabla VIII** se presenta un resumen de los resultados obtenidos al revisar los equipos existentes.

| EQUIPO | SOPORTA IPv6 | VERSIÓN |
|---|---|---|
| ASA 5510 | SI | Cisco ASA Software versión 8.0 |
| Catalyst 4500G | SI | Cisco IOS 12.2 ()SE |
| Catalyst 3750G | SI | Cisco IOS 12.2 ()SE |
| Catalyst 2960G | SI | Cisco IOS 12.2 ()SE |

**TABLA VIII SOPORTE IPV6 EN LOS EQUIPOS DE RED.**

De acuerdo con la información recopilada todos los equipos antes mencionados cuentan con soporte IPv6 a continuación se detallará en la **Tabla IX** las características resumidas en base a los manuales de los propios fabricante.

| EQUIPO | CARACTERISTICAS IPv6 |
|---|---|
| **ASA 5510** | ➢ Provee control de acceso y servicios de firewall para ambientes de redes nativos IPv6 y mixtos (IPv4 & IPv6).<br>➢ Entrega servicios de inspección para aplicaciones basados en HTTP, FTP, SMTP, ICMP, UDP y TCP.<br>➢ Permite la administración remota desde SSHv2, Telnet, HTTP, HTTPS e ICMP corriendo sobre IPv6. |

| | |
|---|---|
| **CATALYST 4500, 3750 y CATALYST 2960** | ➢ Enrutamiento estático.<br>➢ Descubrimiento de máximo MTU.<br>➢ Protocolo de descubrimiento de vecinos.<br>➢ BPG4-MP, EIGRP, OSPFv3 y RIPng.<br>➢ Acceso mediante SSH, HTTPS sobre IPv6.<br>➢ Búsquedas DNS sobre Ipv6.<br>➢ Extended y Standard Access Control List para IPv6.<br>➢ Configuración automática de direcciones.<br>➢ ICMPv6.<br>➢ Soporte CEF/dCEF. |

**TABLA IX SOPORTE IPV6 EN LOS EQUIPOS DE RED.**

Cabe recalcar que CISCO utiliza en sus productos el sistema operativo IOS. Este es un sistema operativo monolítico, lo que significa que corre como una sola instancia y que todos los procesos comparten el mismo espacio de memoria. Por este hecho, errores en una operación pueden tener alterar o corromper otros procesos del sistema. Junto a esto, si un usuario desea agregar nuevas funciones o complementos al sistema operativo, se debe detener el equipo y reemplazar el sistema operativo completamente.

Cisco consciente de estas limitaciones en su sistema operativo, ha desarrollado nuevas versiones del IOS (IOS XR, IOS XE y NX-OS), que buscan superar las limitaciones del esquema monolítico del IOS original. Estos 3 sistemas operativos son de arquitectura modular: los servicios de IOS corren como módulos sobre un núcleo Linux (NX-OS y IOS XE) o un núcleo POSSIX (IOS XR).

## 3.5 SOPORTE IPV6 EN SISTEMAS OPERATIVOS

Fue necesario evaluar el estado actual del soporte IPv6 en los sistemas operativos y aplicaciones utilizados por los usuarios de la red institucional. Se analizaron los principales sistemas operativos utilizados en la actualidad, con el fin de detectar posibles incompatibilidades con el protocolo IPv6.

Prácticamente todos los sistemas operativos desarrollados actualmente cuentan con soporte IPv6. Para las organizaciones y empresas, dicha característica es vista como una garantía de que dichos productos funcionaran adecuadamente en los próximos años. Sin embargo, los ciclos de adopción de los sistemas operativos son extensos, lo que hace necesario revisar el soporte IPv6 en versiones anteriores de dichos sistemas. En la **Tabla X** se presenta un resumen con el soporte IPv6 de los sistemas operativos más utilizados por usuarios y servidores en la red institucional de la UNACH.

| Sistema Operativo | Soporte IPv6 | Observaciones |
|---|---|---|
| Windows 2003 | Sí | |
| Windows Vista | Sí | |
| Windows XP | Sí | |
| Windows 7 | Sí | |
| Windows 2000 | No | Soporte parcial a través de software adicional |
| Windows 95/98 | No | Soporte parcial a través de software adicional |
| Linux | Sí | |

**TABLA X SOPORTE IPV6 EN LOS SISTEMAS OPERATIVOS.**

### 3.5.1 SISTEMAS OPERATIVOS WINDOWS

Microsoft se encuentra trabajando activamente en el desarrollo de integración de IPv6 en sus productos desde la primera publicación oficial del protocolo. Actualmente cuenta con soporte IPv6 en los sistemas operativos Windows XP, Vista, 7, Server 2003 y Server 2008.

Versiones anteriores no cuenta con soporte oficial de Microsoft, sin embargo existen ciertos parches y actualizaciones creadas por terceros que permiten a dichos sistemas contar con un limitado soporte a IPv6. En base al trabajo realizado, se pudieron constatar los siguientes aspectos.

#### 3.5.1.1 Windows XP y Windows Server 2003

- El soporte IPv6 en dichos sistemas debe ser instalado manualmente.
- La dirección del servidor DNS a utilizar debe ser una dirección IPv4. No soportan realizar consultas DNS a través de IPv6.
- No cuentan con una interfaz gráfica para modificar la información IPv6 de una interfaz, se debe utilizar la línea de comandos.
- No soportan el compartir impresoras ni archivos a través de IPv6.
- El firewall incorporado en Windows XP soporta IPv6, pero no se pueden crear reglas específicas para dicho protocolo.
- No soportan IPv6 móvil

#### 3.5.1.2 Windows Vista, Windows 7 y Windows Server 2008

- Estos sistemas operativos cuentan con la última implementación IPv6 desarrollada por Microsoft, la cual incorpora todas las características definidas del protocolo.

- IPv6 es el protocolo capa 3 utilizado por omisión en Windows Vista y Windows 7. Cuando IPv4 e IPv6 se encuentran activados, estos sistemas operativos intentaran conectarse a la dirección IPv6 de un dispositivo remoto.

- Incorporan una interfaz gráfica para la configuración del protocolo.

- Windows 7 incorpora una función denominada Direct Access que proporciona acceso a los recursos de una red a usuarios remotos (similar a una VPN). Es una de las primeras aplicaciones desarrolladas que sólo funciona en IPv6.

### 3.5.2 Linux

Las primeras implementaciones de IPv6 en Linux fueron publicadas el año 1996 y estaban basadas en el proyecto KAME de los sistemas operativos BSD. Uno de los mayores contribuidores al desarrollo IPv6 en Linux es el proyecto USAGI (UniverSAl playGround for Ipv6) manejado por un grupo de voluntarios que buscan implementar todas las funciones de IPv6 en el núcleo de Linux. En Linux cuenta con soporte IPv6 oficialmente desde la versión 2.2. Sin embargo no se recomienda su uso para IPv6, ya que todos los avances y mejoras respecto al protocolo se están realizando en las versiones 2.4.x y 2.6.x.

## 3.6 ANALISIS DE LOS SERVICIOS SOBRE INTERNET QUE BRINDA LA UNACH.

### 3.6.1 Servicio de Resolución de Nombres

El Domain Name System (DNS) es una base de datos distribuida y jerárquica que almacena información asociada a nombres de dominio en redes como Internet. Aunque como base de datos el DNS es capaz de asociar distintos tipos de información a cada nombre, los usos más comunes son la asignación de nombres de dominio a direcciones IP y la localización de los servidores de correo electrónico de cada dominio. Utiliza los puertos 53/UDP, 53/TCP.

Encontramos 3 tipos de DNS:

1.- DNS Primario: el DNS primario solo otorga nombres de dominio, no consulta con otros DNS.

2.- DNS Secundario: el DNS secundario otorga, al igual que el primario, nombres de dominio, pero cuando no se encuentra el nombre de dominio preguntando por el cliente en su servidor consulta a otro DNS.

3.- DNS caché: el DNS cache consulta a otros servidores nombres de dominio.

### 3.6.2 Servicio de Hosting

Un servidor web es un programa que se ejecuta continuamente en un computador, manteniéndose a la espera de peticiones de ejecución que le hará un cliente o un usuario de

Internet. El servidor web se encarga de contestar a estas peticiones de forma adecuada, entregando como resultado una página web textos complejos con enlaces, figuras, formularios, botones y objetos incrustados como animaciones o reproductores de música, o información de todo tipo de acuerdo a los comandos solicitados, usando el protocolo HTTP o el protocolo HTTPS (la versión cifrada y autenticada). El Servicio WEB es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 80 para http y el 443 para HTTPS.

### 3.6.3 Servicio de Correo Electrónico

El correo electrónico o e-mail (acrónimo de Electronic Mail) es el sistema de intercambio de mensajes entre usuarios conectados a una red electrónica. Sirve para enviar mensajes entre usuarios conectados a la misma red, o entre usuarios que tienen sus máquinas conectadas a la Red Internet. Este intercambio de mensajes entre una o varias personas se produce de forma asíncrona, por lo que no se requiere la presencia simultánea de los comunicantes.
Para lograr la conexión se definen una serie de protocolos, cada uno con una finalidad concreta:

- SMTP, Simple Mail Transfer Protocol: Es el protocolo que se utiliza para que dos servidores de correo intercambien mensajes, utilizando el puerto 25.

- POP, Post Office Protocol: Se utiliza para obtener los mensajes guardados en el servidor y pasárselos al usuario, utilizando el puerto 110.

- IMAP, Internet Message Access Protocol: Su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes, utilizando el puerto 110.

### 3.6.4 Servicio de Proxy

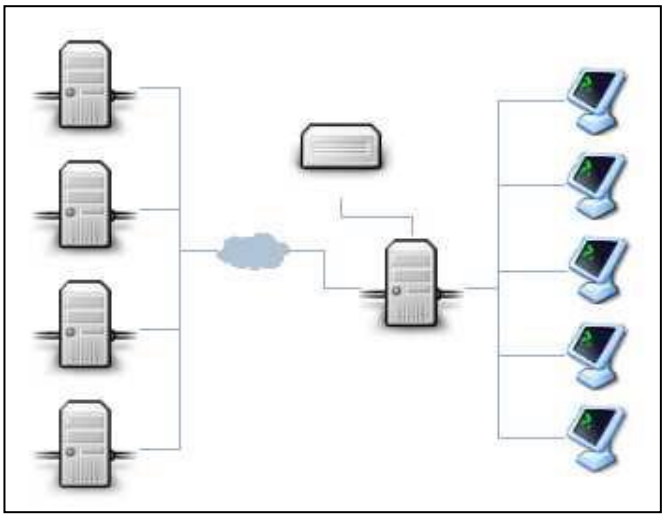


**FIGURA 3.5 SERVICIO DE PROXY[29]**

Un servidor Proxy es un equipo que actúa de intermediario entre un explorador Web (como Internet Explorer, FireFox) e Internet. Los servidores Proxy ayudan a mejorar el rendimiento en Internet ya que almacenan una copia de las páginas web más utilizadas.
Cuando un explorador solicita una página web almacenada en la colección (su caché) del servidor Proxy, el servidor Proxy la proporciona, lo que resulta más rápido que consultar la Web.

Los servidores Proxy también ayudan a mejorar la seguridad, ya que filtran algunos contenidos Web y software malintencionado. También sirve para compartir Internet.

[29] Fuente: http://es.wikipedia.org/wiki/Internet

### 3.6.5 Servicio de Configuración Dinámica de Host

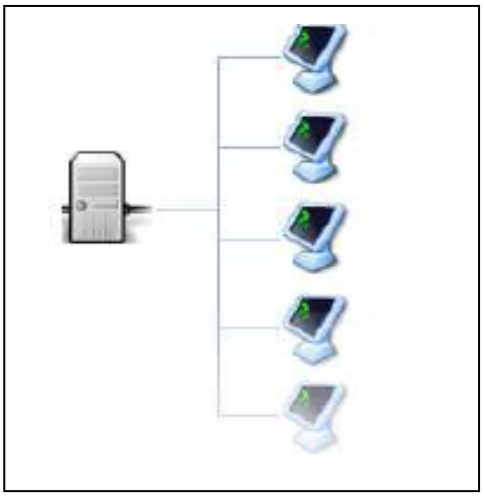


**FIGURA 3.6 SERVICIO DE CONFIGURACIÓN DINÁMICA DE HOST[30]**

DHCP (sigla en inglés de Dynamic Host Configuration Protocol – Protocolo Configuración Dinámica de Anfitrión) es un protocolo de red que permite a los nodos de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

[30] Fuente: http://es.wikipedia.org/wiki/Internet

### 3.6.6 Servicio de Transferencia de Archivos

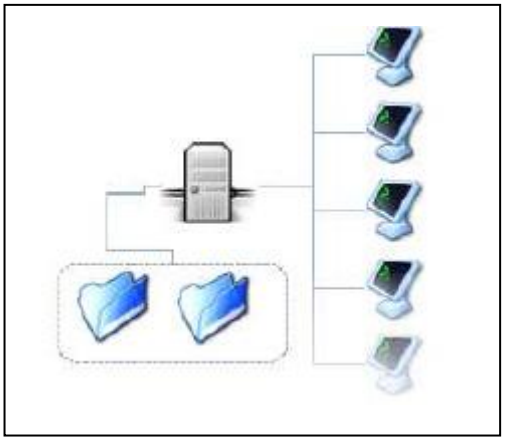


**FIGURA 3.7 SERVICIO DE TRANSFERENCIA DE ARCHIVOS[31]**

En servidor FTP es un servidor que opera sobre el protocolo de transferencia de archivos FTP (File Transfer Protocol por sus siglas en inglés).

Es un protocolo muy común que se ha utilizado durante tanto tiempo como HTTP para transferir archivos en Internet y entre nodos de las redes.

El Servicio FTP es ofrecido por la capa de Aplicación del modelo de capas de red TCP/IP al usuario, utilizando normalmente el puerto de red 20 y el 21.

[31] Fuente: http://es.wikipedia.org/wiki/Internet

### 3.6.7 Servicio de Acceso Remoto

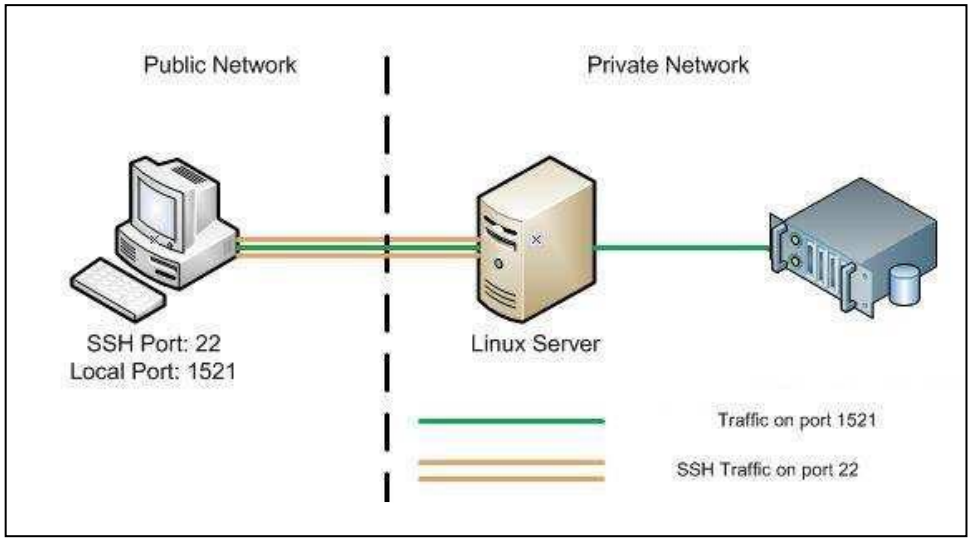



**FIGURA 3.8 SERVICIO DE ACCESO REMOTO**[32]

Telnet (Telecommunication NETwork) es el nombre de un protocolo de red (y del programa informático que implementa el cliente), que sirve para acceder mediante una red a otra máquina, para manejarla remotamente como si estuviéramos sentados delante de ella. Para que la conexión funcione, como en todos los servicios de Internet, la máquina a la que se acceda debe tener un programa especial que reciba y gestione las conexiones.
SSH (Secure SHell) es un protocolo similar a Telnet que permite abrir un shell en una máquina remota, con la diferencia de que SSH encripta toda la información que viaja por la red.

La información mostrada anteriormente se obtuvo del Centro de Cómputo de la UNACH, el mismo que facilitará la implementación con el nuevo protocolo IPv6 en los servicios DNS y WEB. Por lo que el servidor DNS será configurado en Linux y en el servidor WEB la transición al protocolo IPv6 se realizará en el sistema operativo Windows server 2003.

[32] Fuente: http://es.wikipedia.org/wiki/Internet

# CAPITULO IV

# 4. DESARROLLO

## 4.1 ANÁLISIS Y ELECCIÓN DE LA ESTRATEGIA DE TRANSICIÓN MÁS ADECUADA.

Migrar hacia IPv6 puede ser complejo en organizaciones grandes, pero las estrategias existentes pueden ayudar mucho a facilitar esta transición. Estos mecanismos no son alternativas a otros, pero en cualquier caso, requieren conocer a fondo nuestra infraestructura, para así poder seleccionar la estrategia más apropiada para lograr nuestro objetivo. Para la mayoría de nosotros, ese objetivo es migrar a IPv6 con costos bajos y que el impacto sea mínimo.

Para la elección de que mecanismo implementar se ha resumido en el siguiente cuadro los aspectos más importantes de los mecanismos.

| **MECANISMOS DE TRANSICIÓN** | |
|---|---|
| Dual Stack | ➢ Es fácil implementar.<br>➢ Es la solución inmediata más accesible.<br>➢ Permite que los nuevos dispositivos IPv6 relacionarse rápidamente con el resto de los dispositivos. |
| Tunnels | ➢ Para configurar un túnel se necesita saber cuatro cosas esenciales: la dirección ipv4 de origen y destino que serán utilizados para la |

| | |
|---|---|
| | encapsulación, y las direcciones ipv6 que se utilizaran para realizar la conexión punto a punto.<br>➢ Necesitaremos contar con dual stack en cada uno de los puntos del túnel.<br>➢ El mecanismo para la implementación de túneles varía de una plataforma a otra.<br>➢ Requiere más configuración que los otros métodos. |
| Translators | ➢ Adolece los mismos problemas de NAT IPv4.<br>➢ Fiabilidad<br>➢ Cuello de botella<br>➢ Incompatibilidad en distintas aplicaciones.<br>➢ Escalabilidad<br>➢ Se pierden los beneficios de ipv6. |

**TABLA XI MECANISMOS DE TRANSICIÓN**

## 4.2. MECANISMO DE IMPLEMENTACIÓN DE LA RED IPV6

Con el análisis anterior se ha concluido que el mecanismo de transición mas óptimo para la implementación de la red IPv6, sobre la red de la Universidad Nacional de Chimborazo, que funciona sobre IPv4, es factible utilizar la técnica del Dual Stack, que permita

mantener funcionando el actual protocolo simultáneamente con la nueva tecnología, de manera que se garantice la conectividad de los nodos de la red y cuando no sea posible utilizar IPv6, se puede utilizar IPv4.

Las desventajas serían una disminución del desempeño de los equipos de red, que deben mantener tablas de direcciones y rutas independientes para cada protocolo.

## 4.3 IMPLEMENTACIÓN DE LA DIRECCIÓN IPv6

La Universidad Nacional de Chimborazo, forma parte del Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA), el cual se encarga de asignar direcciones IPv6 a todas las universidades que se encuentran en el gran reto de transición a este nuevo protocolo de versión 6. El prefijo IPv6 que se le fue asignada a la UNACH es:

2800:0068:000b::/48

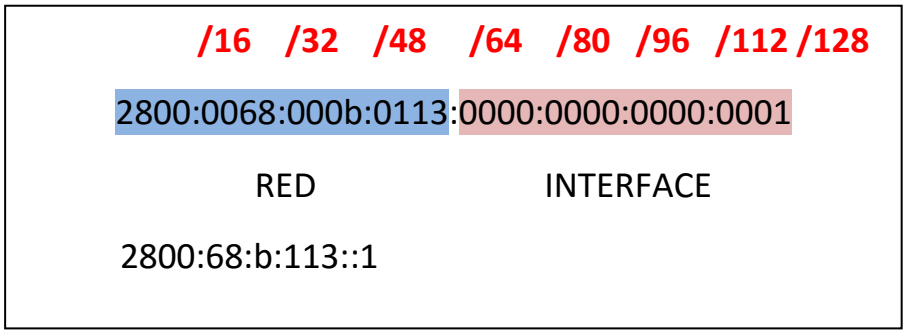



**FIGURA 4.1 REPRESENTACIÓN DE LA RED E INTERFACE (DIRECCIÓN IPV6 DMZ)**

- Los primeros 32 bits ( 8 hexadecimales ) definen la red de CEDIA ▸2800:68
- Los siguientes 16 bits (4 hexadecimales ) definen la red de la Universidad ▸000B:

- Los siguientes 16 bits (4 hexadecimales) definen a cada una de las redes de la Universidad ►:0113:
- Los últimos 64 bits (16 hexadecimales ) son los que definen a un host especifico► :0000:0000:0000:0001

### 4.3.1 IMPLEMENTACIÓN DUAL STACK

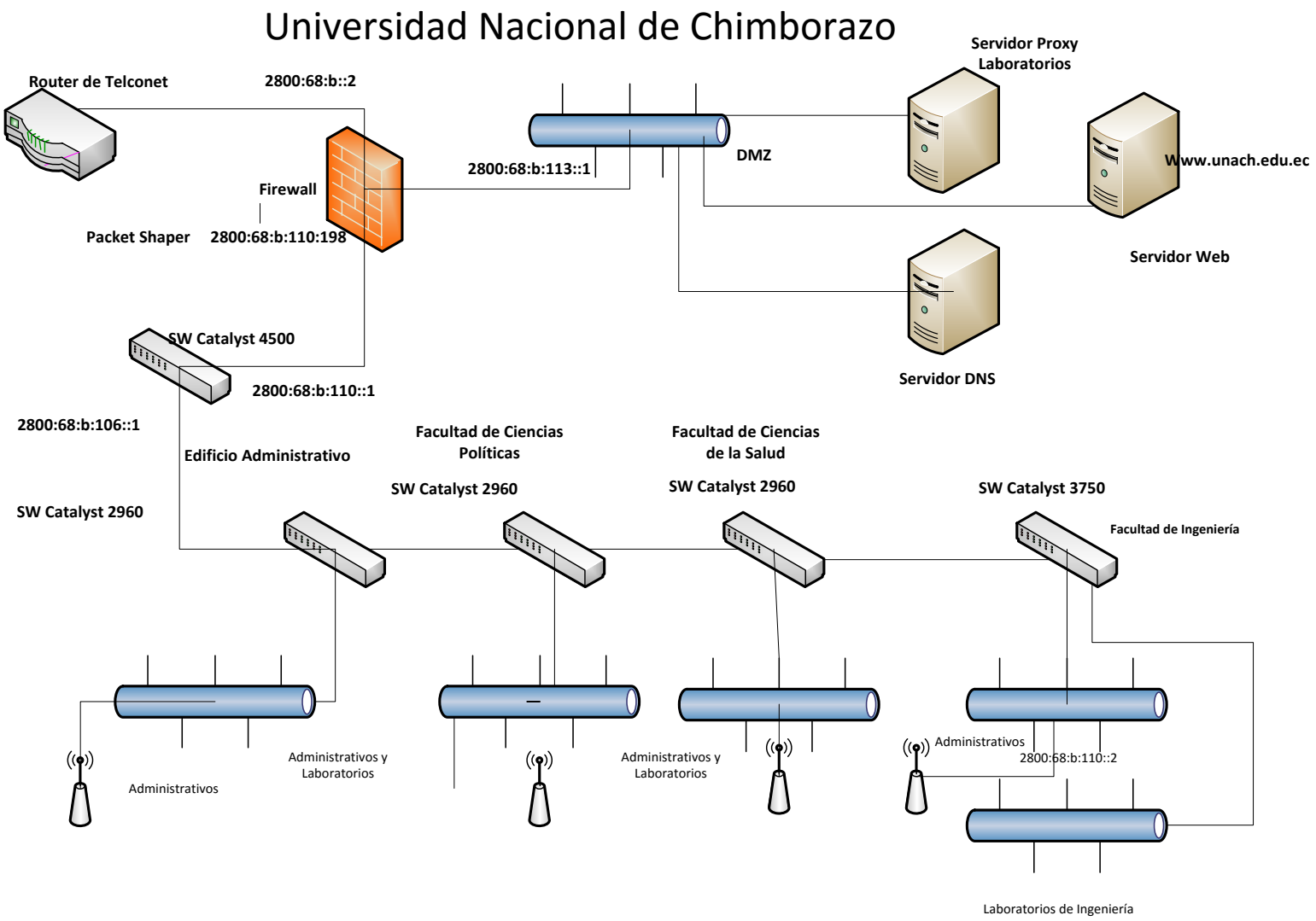
Según lo mencionado anteriormente para nuestra facilidad y la del administrador de red para la asignación de direcciones IPv6 utilizamos las mismas VLANs que son empleadas en IPv4 ya que evitará confusiones en la implementación de futuras direcciones, es decir se usará la dirección asignada por CEDIA y las VLANS de IPv4 que representan a cada facultad y departamentos de la UNACH como se muestra en la siguiente tabla.

| **Implementación Dual Stack (DOBLE PILA IPv4/IPv6)** | | |
|---|---|---|
| **NOMBRE DE LA VLAN** | **DIRECCION IPv4** | **DIRECCION IPv6** |
| | **IP/MÁSCARA** | **IP/MÁSCARA** |
| Financiero | 192.168.102.0/24 | 2800:0068:000b:102::/64 |
| Administrativo | 192.168.110.0/24 | 2800:0068:000b:110::/64 |
| DMZ | 192.168.113.0/24 | 2800:0068:000b:113::/64 |
| Departamento de Evaluación | 192.168.128.0/24 | 2800:0068:000b:128::/64 |
| Cisco Inalámbrico | 192.168.123.0/24 | 2800:0068:000b:123::/64 |
| Wireless T.PLINK | 192.168.124.0/24 | 2800:0068:000b:124::/64 |
| Wireless Lan Controler | 192.168.120.0/24 | 2800:0068:000b:120::/64 |

| | | |
|---|---|---|
| F. Ingeniería | 192.168.106.0/24 | 2800:0068:000b:106::/64 |
| F. Ciencias de la Salud | 192.168.107.0/24 | 2800:0068:000b:107::/64 |
| F. Ciencias Políticas. | 192.168.111.0/24 | 2800:0068:000b:111::/64 |
| | **CAMPUS LA DOLOROSA** | |
| F. Ciencias de la Educación | 192.168.103.0/24 | 2800:0068:000b:103::/64 |
| Psicología | 192.168.104.0/24 | 2800:0068:000b:104::/64 |
| Wireless T.PLINK | 192.168.126.0/24 | 2800:0068:000b:126::/64 |
| Wireless Lan Controler | 192.168.125.0/24 | 2800:0068:000b:125::/64 |
| Administración | 192.168.112.0/24 | 2800:0068:000b:112::/64 |

**TABLA XII** DIRECCIONAMIENTO INTERNO.

## 4.4 TOPOLOGÍA ACTUAL CON EL DIRECCIONAMIENTO IPv6



## 4.5 DIRECCIONAMIENTO

### 4.5.1 Direccionamiento IPv6 en la UNACH

Para la configuración de las direcciones IPv6 de los nodos se determinó conveniente utilizar el mecanismo de autoconfiguración existente en IPv6. Donde la dirección asignada a cada host se la recalizara mediante el mecanismo RADV incluido en la versión IOS del switch de CORE.

La excepción la constituyen los servidores y equipamiento de red ("switch", "router", "firewall"), a los cuales se les asignará su dirección IPv6 de forma manual para garantizar la seguridad y optimizar la administración.

### 4.5.2 Protocolo de enrutamiento en la Red Institucional

Para implementar IPv6, se utilizará enrutamiento estático entre las VLAN's existentes en la Universidad Nacional de Chimborazo que facilitará asignar las rutas manualmente a la red.

### 4.5.3 Configuración del Switch

Una vez que se ingresa al switch se procede a crear una interface o trabajar en las ya existentes en IPv4 como se muestra a continuación utilizando varios comandos:

| | |
|---|---|
| Switch # configure terminal | Modo de Configuración |
| Switch(config)# interface vlan 80 | Crea una interface en la VLAV 80 |
| Switch(config-if)# ipv6 enable | Habilita IPv6 |
| Switch(config-if)# ipv6 address 2800:68:b:80::1/64 | Asigna la dirección IPv6 a la VLAN |
| Switch(config-if)# no shutdown | Levanta la Interface |
| Switch(config-if)# end | Finaliza el proceso |
| Switch # show run | muestra todas las interfaces existentes |

**TABLA XIII. CONFIGURACIÓN VLAN's**

### 4.5.4 Configuración del Switch 4500 (Telnet 192.168.112.65)

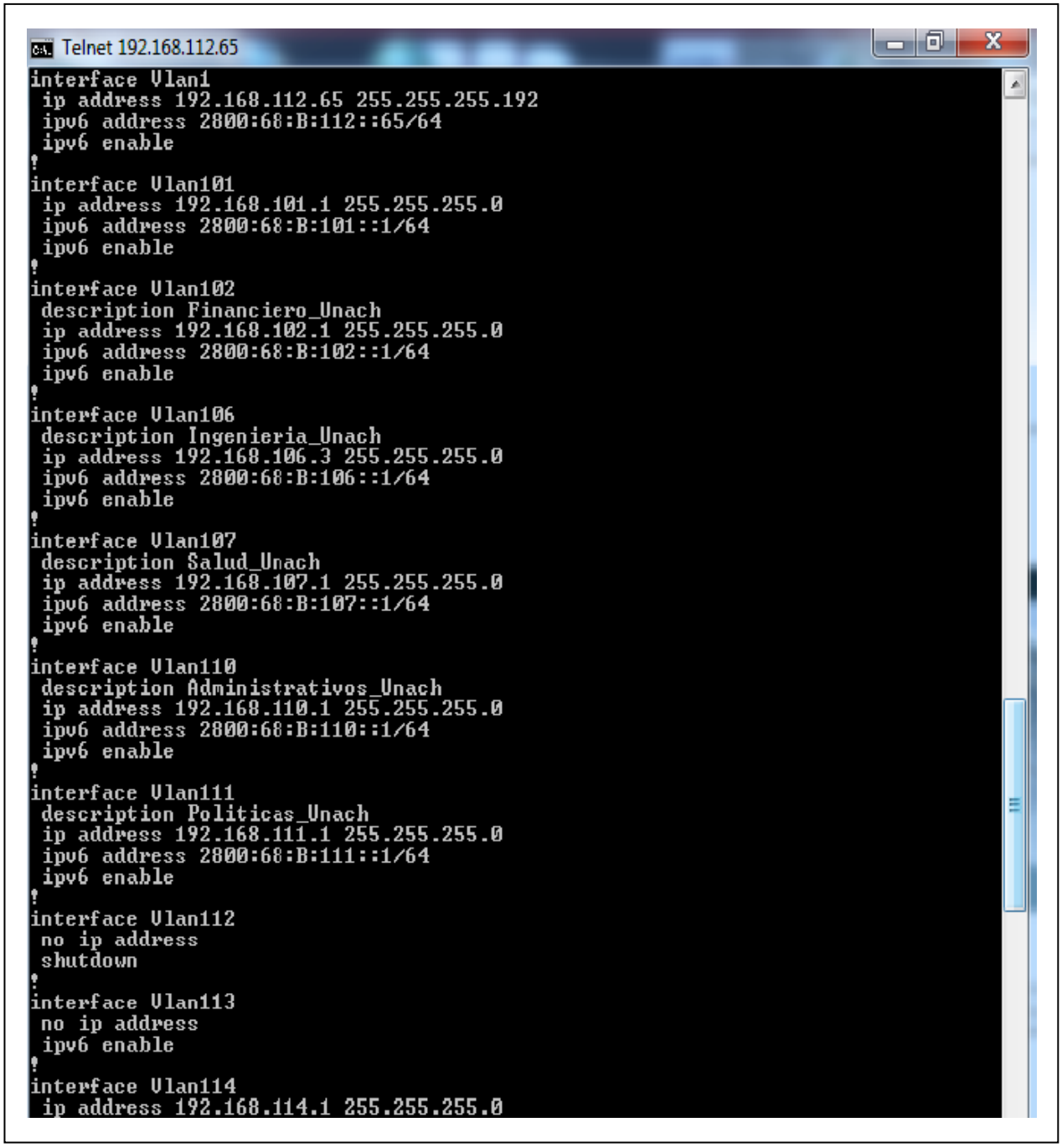
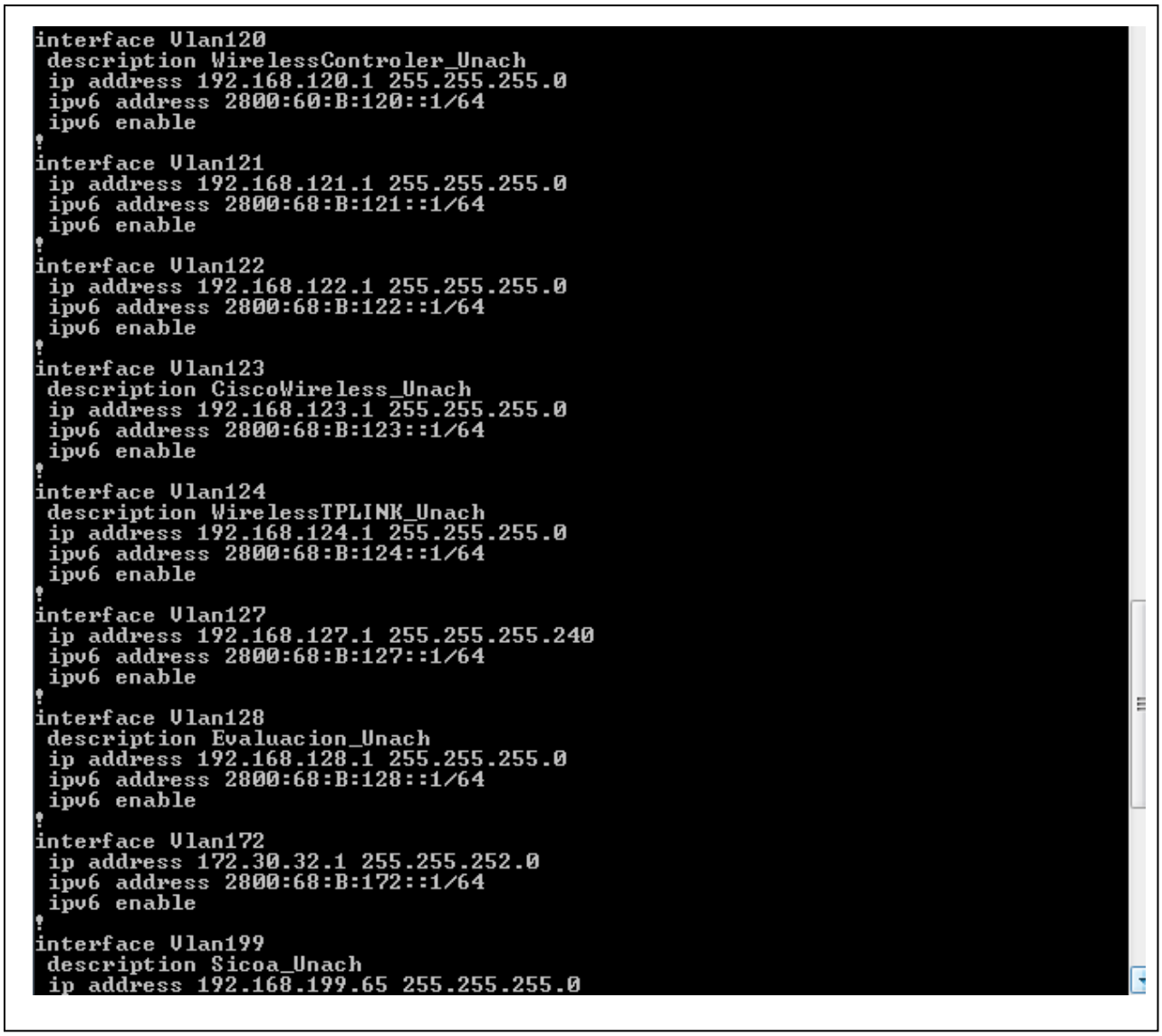



**FIGURA 4.3 COFIGURACIÓN DE LAS VLAN'S EN IPV6**



```
interface Vlan120
 description WirelessControler_Unach
 ip address 192.168.120.1 255.255.255.0
 ipv6 address 2800:60:B:120::1/64
 ipv6 enable
!
interface Vlan121
 ip address 192.168.121.1 255.255.255.0
 ipv6 address 2800:68:B:121::1/64
 ipv6 enable
!
interface Vlan122
 ip address 192.168.122.1 255.255.255.0
 ipv6 address 2800:68:B:122::1/64
 ipv6 enable
!
interface Vlan123
 description CiscoWireless_Unach
 ip address 192.168.123.1 255.255.255.0
 ipv6 address 2800:68:B:123::1/64
 ipv6 enable
!
interface Vlan124
 description WirelessTPLINK_Unach
 ip address 192.168.124.1 255.255.255.0
 ipv6 address 2800:68:B:124::1/64
 ipv6 enable
!
interface Vlan127
 ip address 192.168.127.1 255.255.255.240
 ipv6 address 2800:68:B:127::1/64
 ipv6 enable
!
interface Vlan128
 description Evaluacion_Unach
 ip address 192.168.128.1 255.255.255.0
 ipv6 address 2800:68:B:128::1/64
 ipv6 enable
!
interface Vlan172
 ip address 172.30.32.1 255.255.252.0
 ipv6 address 2800:68:B:172::1/64
 ipv6 enable
!
interface Vlan199
 description Sicoa_Unach
 ip address 192.168.199.65 255.255.255.0
```

**FIGURA 4.3 COFIGURACIÓN DE LAS VLAN'S EN IPV6**

### 4.5.5. Configuración de las puertas de enlace en el FIREWALL Institucional

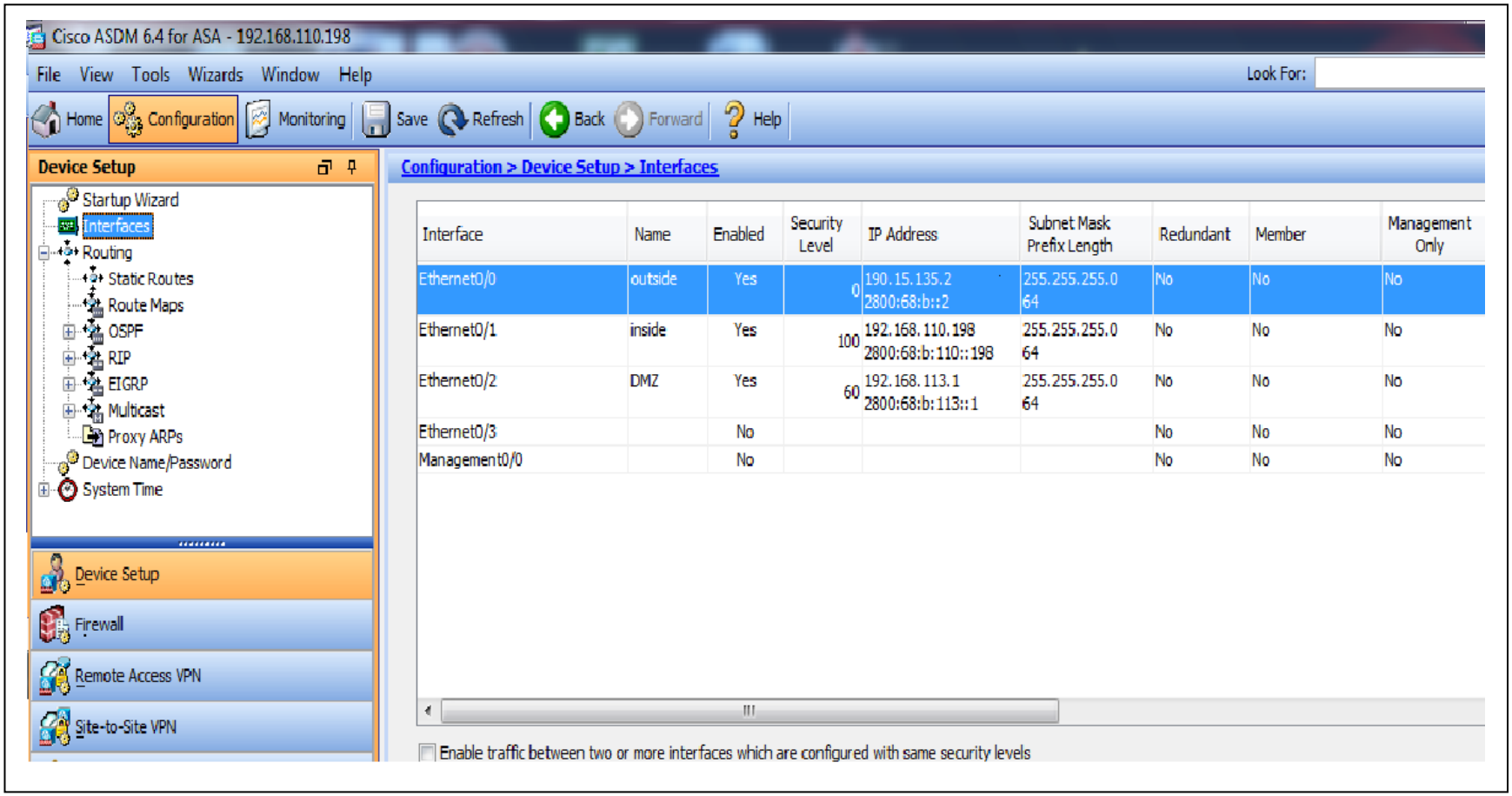



**FIGURA 4.4 ASA 192.168.110.198**

### 4.5.6 Reglas de acceso en el Firewall interno Institucional

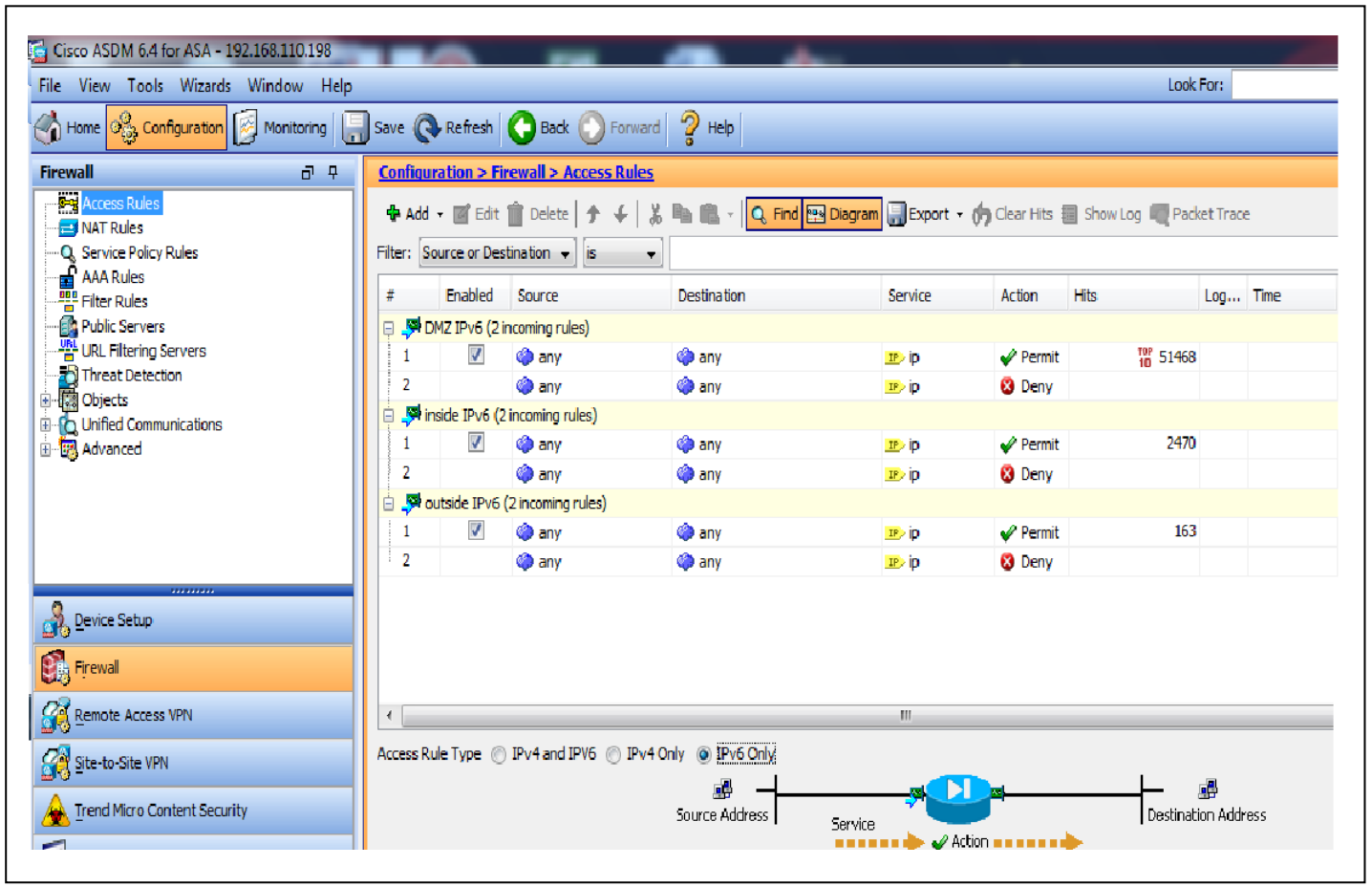
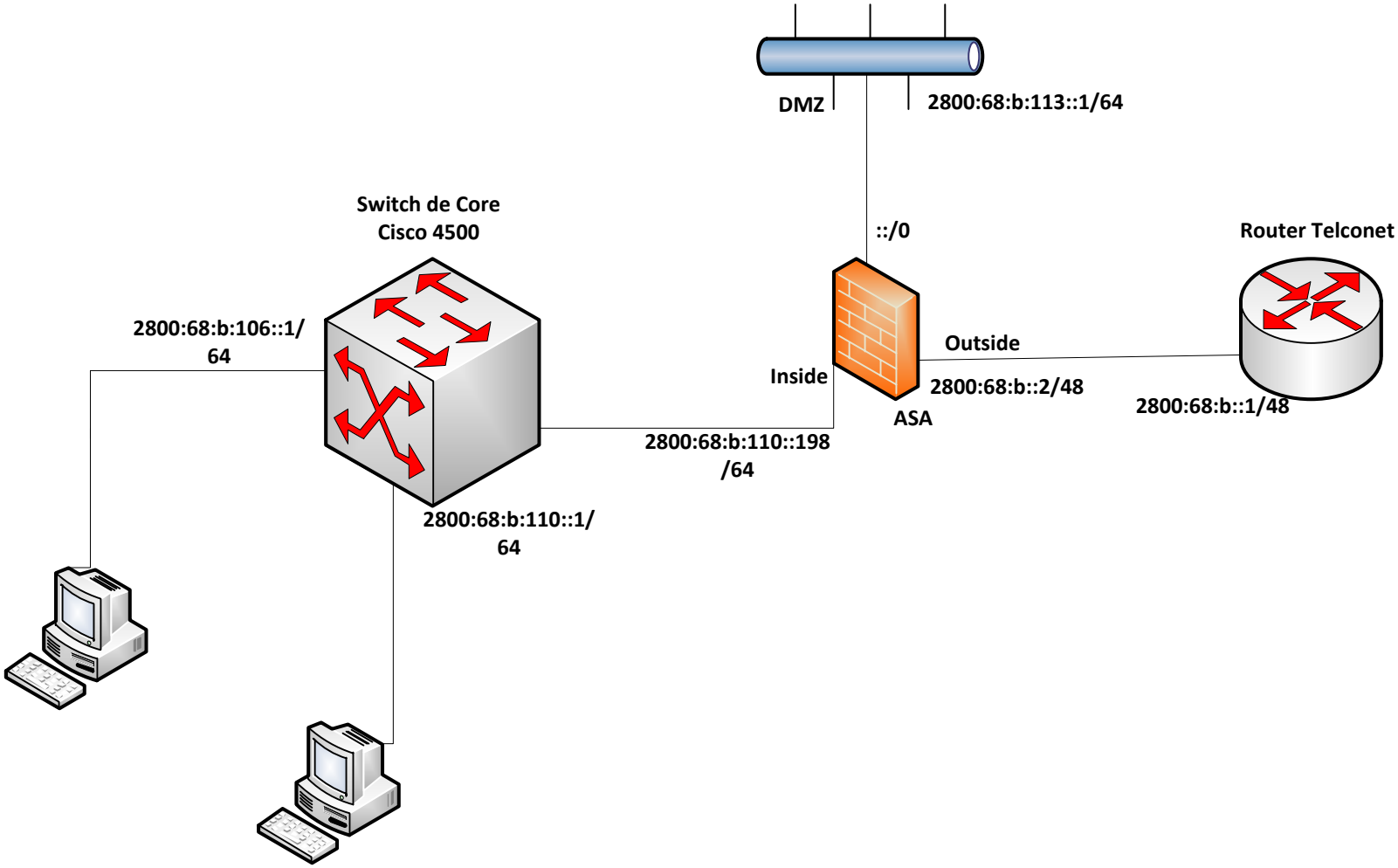



**FIGURA 4.5 REGLAS DE ACCESO**

### 4.5.7 Salida de las direcciones de IPv6 Hacia el Internet



## 4.6 CONFIGURACIÓN DE LOS SERVIDORES

Para realizar la configuración de los servidores DNS, WEB y PROXY utilizamos el programa gratuito PUTTY, que por medio del mismo realizamos conexiones a distintos servidores y protocolos como SSH Y TELNET estos protocolos sirven básicamente para conectarse remotamente a otros equipos de tipo servidores que usan esas tecnologías. El protocolo que fue usado fue el SSH.

### 4.6.1 SERVIDOR DEL SISTEMA DE NOMBRES DE DOMINIO (DNS)

Una vez instalado el Putty colocamos la dirección IP donde se encuentra el servidor DNS.

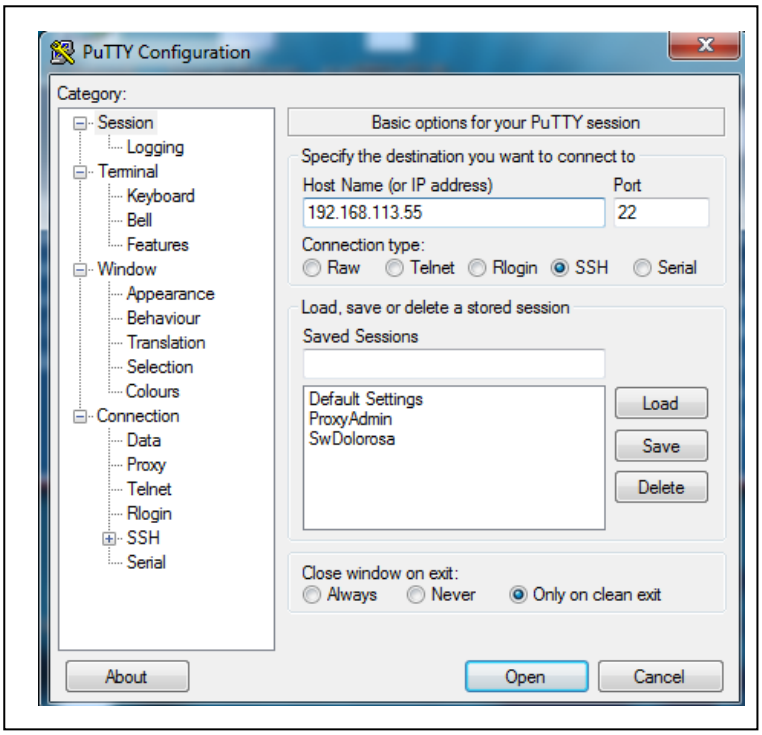



**FIGURA 4.6 PANTALLA INICIAL**

Al ingresar al servidor nos despliega una pantalla en la cual se nos pide un usuario y por ende una contraseña una vez ingresado al servidor DNS iniciamos las respectivas configuraciones.

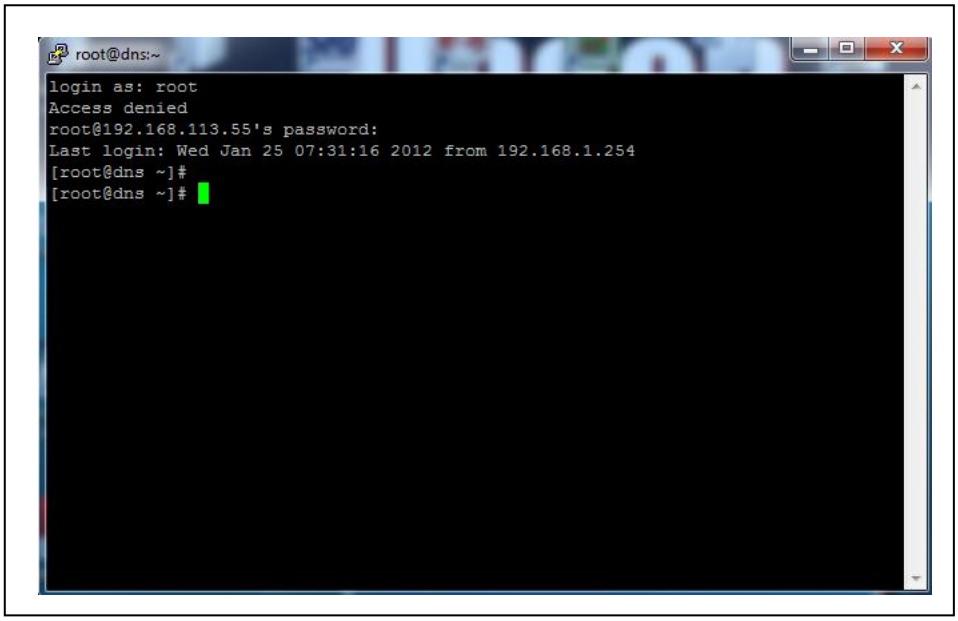



**FIGURA 4.7 SERVIDOR DNS**

### 4.6.1.1 Activar Ipv6

El archivo /etc/sysconfig/network es usado para especificar la información sobre la configuración de la red deseada.

**NETWORKING=<valor>**

Donde <valor> es uno de los siguientes valores booleanos:

yes = Se debería configurar el servicio de red.

**NETWORKING=IPV6<valor>**

Donde <valor> es uno de los siguientes valores booleanos:

yes = Habilita ipv6.

No = No habilita ipv6.

**HOSTNAME=<valor>**

Donde <valor> debería ser el Fully Qualified Domain Name (FQDN), nombre de dominio cualificado completo, tal como

hostname.expample.com, pero puede ser cualquier nombre de host necesario.

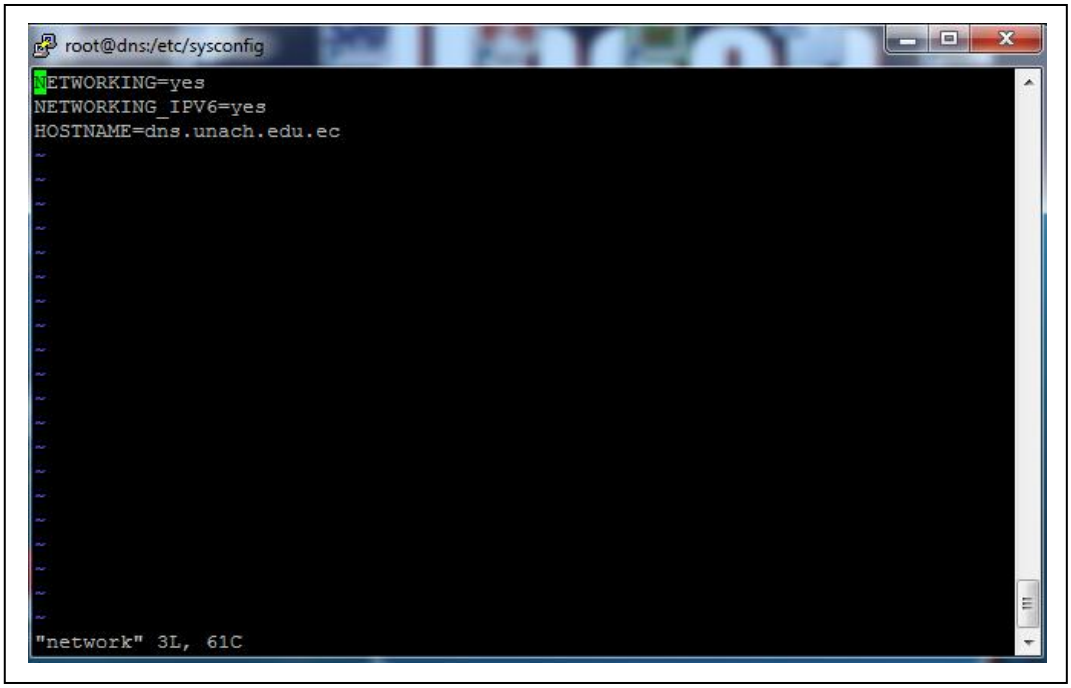



**FIGURA 4.8 /etc/sysconfig/network**

Los archivos de configuración de interfaz controlan las interfaces de software para dispositivos de red individuales. Cuando su sistema arranca, utiliza estos archivos para saber qué interfaces debe activar y cómo deben ser configuradas. Estos archivos habitualmente se conocen como ifcfg-<*nombre*>, donde <*nombre*> hace referencia al nombre del dispositivo que controla el archivo de configuración, cada interfaz de red configurada, tal como ifcfg-eth0 para la interfaz de red Ethernet eth0.

**DEVICE=<nombre>**

Donde <nombre> es el nombre del dispositivo físico (a excepción de los dispositivos PPP asignados de forma dinámica en donde éste es el nombre lógico).

**BOOTPROTO=<protocolo>**

Donde <protocolo> es uno de los siguientes:
none = No se debería utilizar ningún protocolo de tiempo de arranque.
Bootp = Se debería utilizar el protocolo BOOTP.
Dhcp = Se debería utilizar el protocolo DHCP.

**HWADDR=<dirección-MAC>**

Donde <dirección-MAC> es la dirección de hardware del dispositivo Ethernet en la forma de AA:BB:CC:DD:EE:FF. Esta directriz es útil en las máquinas con múltiples NICs para asegurarse de que a las interfaces se les asignen los nombres correctos de dispositivos sin importar el orden de carga configurado para cada módulo NIC. Esta directriz no debería ser usada en conjunto con MACADDR.

**ONBOOT=<respuesta>**

Donde <respuesta> es una de las siguientes:
yes = El dispositivo debería activarse en el momento de arranque.
no = Este dispositivo no debería activarse en el momento de arranque.

**TYPE=<nombre>**

Donde <respuesta> es Ethernet

**USERCTL=<respuesta>**

Donde <respuesta> es una de las siguientes:
yes = Los usuarios que no sean root pueden controlar este dispositivo.
no = No se les permite controlar este dispositivo a los usuarios que no sean root.

**IPV6INIT=<respuesta>**

Donde <respuesta> es una de las siguientes:
yes = Habilita ipv6 en esta interfaz.
no = No habilita ipv6 en esta interfaz.

**IPV6ADDR=<dirección>**

Donde <dirección> es la dirección IPv6.

**PEERDNS=<respuesta>**

Donde <respuesta> es una de las siguientes:

yes = Modifica /etc/resolv.conf si está activada la directriz DNS. Si está usando DCHP, la opción yes es la predeterminada.
no = No modificar /etc/resolv.conf.

**IPADDR=<dirección>**

Donde <dirección> es la dirección IP.

**NETMASK=<máscara>**

Donde <máscara> es el valor de la máscara de red.

**GATEWAY=<dirección>**

Donde <dirección> es la dirección IPv4 del enrutador o dispositivo de puerta de enlace (si existe).

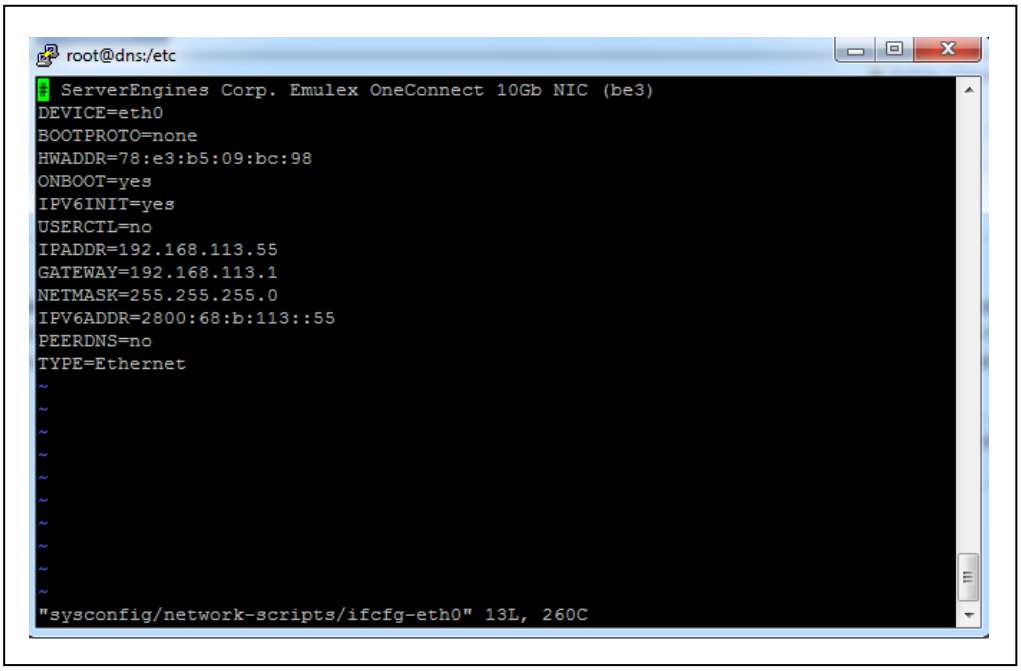



**FIGURA 4.9 etc/sysconfig/network-scripts/ifcfg-eth0**

### 4.6.1.2 Configuración de hosts

Cuando el sistema intente resolver un nombre de host a una dirección IP, o de determinar el nombre de host para una dirección IP, hará referencia al archivo /etc/hosts antes de usar los servidores de nombres. Si aparece la dirección IP en el archivo /etc/hosts, no se utilizarán los servidores de nombres. Si la red contiene ordenadores cuyas direcciones IP no aparecen en DNS, se recomienda añadirlas al archivo /etc/hosts.

La sintaxis es:

<dirección IP> < nombre de dominio cualificado (FQDN)> < alias>

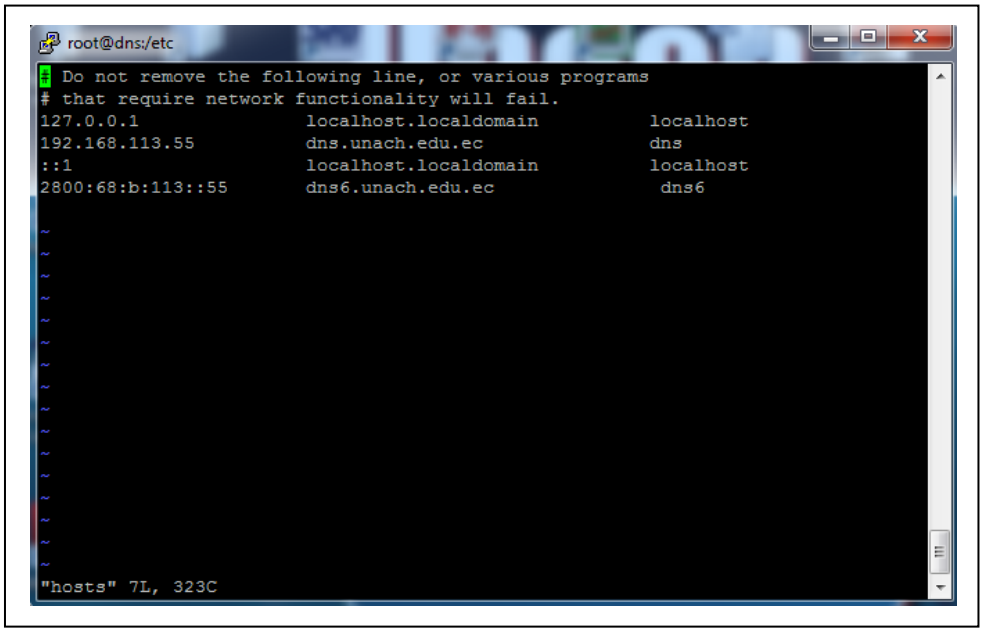



**FIGURA 4.10 /etc/hosts**

El archivo host.conf determina el orden de llamada a los servicios de resolución de nombres. Los parámetros posibles, separados por espacios o comas, son:

- **hosts:** Búsqueda en el archivo /etc/hosts
- **bind:** Llamada a un servidor de nombres

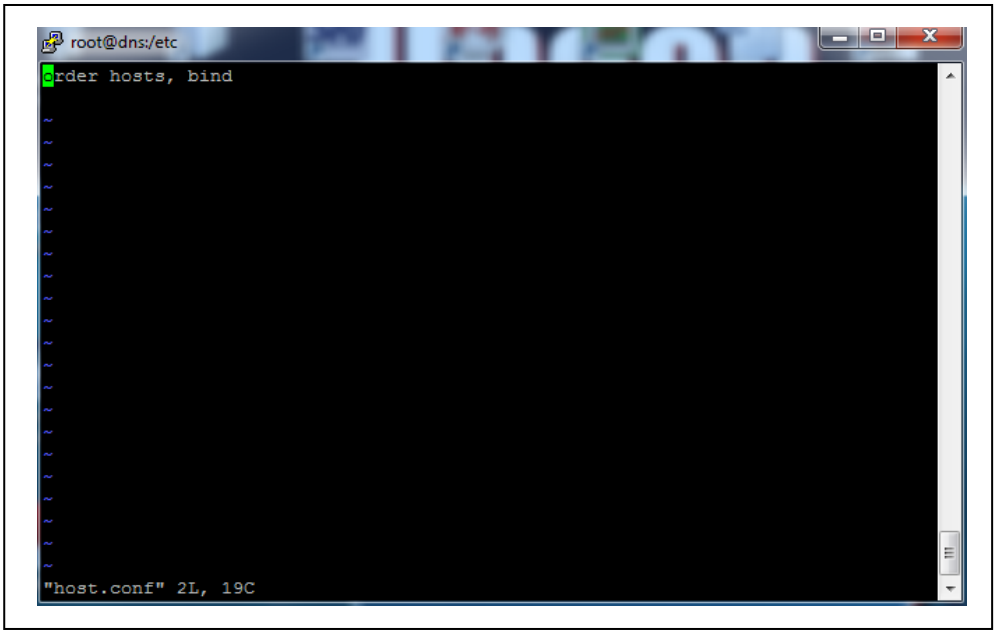



**FIGURA 4.11 /etc/host.conf**

#### 4.6.1.3 Archivos de Configuración del DNS

El archivo named.conf es una colección de declaraciones que utilizan opciones anidadas rodeadas por corchetes, { } y son las siguientes.

##### 4.6.1.3.1 Declaración options

La declaración options define opciones de configuración de servidor globales y configura otras declaraciones por defecto. Puede ser usado para especificar la ubicación del directorio de trabajo named, los tipos de consulta permitidos y más.

- **listen-on**

  Especifica la interfaz de red en la cual named escucha por solicitudes. Por defecto, todas las interfaces son usadas.
  Al usar esta directiva en un servidor DNS que también actúa como un gateway, BIND puede ser configurado para sólo contestar solicitudes que se originan desde algunas de las redes.

- **query-source**

  Indica a BIND qué puerto usar para las consultas.

Las directivas que se muestran en la Figura 4.12 son las que hacen posible la implementación Doble Pila IPv4/IPv6.

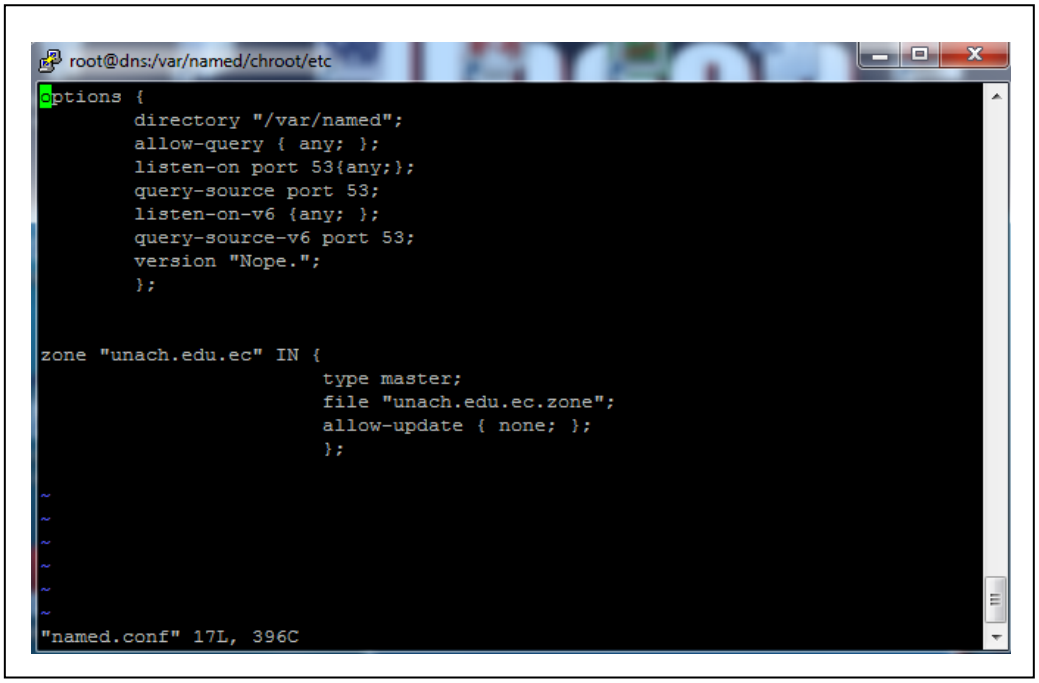



**FIGURA 4.12 /var/named/chroot/etc/named.conf**

#### 4.6.1.3.2 Archivos de zona

Los Archivos de zona contienen información sobre un espacio de nombres particular. Estos son almacenados en el directorio de trabajo named, por defecto /var/named/. Cada archivo de zona es nombrado de acuerdo a la opción file en la declaración zone, usualmente en una forma que relaciona al dominio en cuestión e identifica el archivo como un archivo que contiene datos de zona.

##### 4.6.1.3.2.1 Declaración zone

Una declaración zone define las características de una zona, tal como la ubicación de su archivo de configuración y opciones específicas de la zona, sus directivas son:

- **type**

Define el tipo de zona.

master = Designa el servidor de nombres actual como el servidor autoritativo para esa zona. Una zona se puede configurar como tipo master si los archivos de configuración de la zona residen en el sistema.

slave = Designa el servidor de nombres como un servidor esclavo para esa zona. También especifica la dirección IP del servidor de nombres maestro para la zona.

- **File**

  Especifica el nombre del archivo en el directorio de trabajo named que contiene los datos de configuración de zona.

- **allow-update**

  Especifica los hosts que están autorizados para actualizar dinámicamente la información en sus zonas. Por defecto, no se autoriza la actualización dinámica de la información.

  Tenga cuidado cuando autorice a los hosts para actualizar la información de su zona. No habilite esta opción si no tiene confianza en el host que vaya a usar. Es mejor que el administrador actualice manualmente los registros de zona y que vuelva a cargar el servicio named.

Como se en la figura 00 la zona es identificada como unach.edu.ec, el tipo es configurado a master y el servicio named se instruye para leer el archivo /var/named/unach.edu.ec.zone.

También le dice a named que no permita a ningún otro host que realice actualizaciones.

Una declaración zone de servidor esclavo para unach.edu.ec se ve un poco diferente comparado con el ejemplo anterior. Para un servidor esclavo, el tipo se coloca a slave y en lugar de la línea allow-update está una directiva diciéndole a named la dirección IP del servidor maestro.

Los mismos parámetros para la zona de resolución inversa.
Una vez configurado el archivo named.conf, se procede a configurar y crear los archivos de zonas ubicados en /var/named/chroot/var/named/.

#### 4.6.1.3.2.2 Registros de recursos de archivos de zona

El componente principal de un archivo de zona es su registro de recursos.
Hay muchos tipos de registros de recursos de archivos de zona. A continuación les mostramos los tipos de registros más frecuentes:

- **$INCLUDE**

  Configura a named para que incluya otro archivo de zona en el archivo de zona donde se usa la directiva. Así se pueden almacenar configuraciones de zona suplementarias aparte del archivo de zona principal.

- **$TTL**

  Ajusta el valor Time to Live (TTL) predeterminado para la zona. Este es el tiempo, en segundos, que un registro de recurso de zona es válido. Cada recurso puede contener su propio valor TTL, el cual ignora esta directiva.

  Cuando se decide aumentar este valor, permite a los servidores de nombres remotos hacer caché a la información de zona para un período más largo de tiempo, reduciendo el número de consultas para la zona y alargando la cantidad de tiempo requerido para proliferar cambios de registros de recursos.

- **A**

  Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv4 de 32 bits., como en el siguiente ejemplo:

<host> IN A <IP-address>

Si el valor <host> es omitido, el registro A apunta a una dirección IP por defecto para la parte superior del espacio de nombres. Este sistema es el objetivo para todas las peticiones no FQDN.

- **AAAA**

  Registro de dirección que resuelve un nombre de un anfitrión hacia una dirección IPv6 de 128 bits.

- **CNAME**

  Se refiere al Registro del nombre canónico, el cual enlaza un nombre con otro. Esta clase de registros es también conocida como un alias record.

  El próximo ejemplo indica a named que cualquier petición enviada a <aliasname> apuntará al host, <real-name>. Los registros CNAME son usados normalmente para apuntar a servicios que usan un esquema de nombres común, tal como www para servidores Web.

  <alias-name> IN CNAME <real-name>

- **MX**

  Registro de Mail eXchange, el cual indica dónde debería ir el correo enviado a un espacio de nombres particular controlado por esta zona.

  IN MX <preference-value><email-server-name>

  En este ejemplo, <preference-value> permite una clasificación numérica de los servidores de correo para un espacio de nombres, dando preferencia a algunos sistemas de correo sobre otros. El registro de recursos MX con el valor más bajo <preference-value> es preferido sobre los otros. Sin embargo, múltiples servidores de correo pueden tener el mismo valor para distribuir el tráfico de forma pareja entre ellos.

  El <email-server-name> puede ser un nombre de servidor o FQDN.

  IN MX 10 mail.example.com. IN MX 20 mail2.example.com.

En este ejemplo, el primer servidor de correo mail.example.com es preferido al servidor de correo mail2.example.com cuando se recibe correo destinado para el dominio example.com.

- **NS**

  Se refiere al Registro NameServer, el cual anuncia los nombres de servidores con autoridad para una zona particular.
  El siguiente ejemplo es un ejemplo de un registro NS:
  IN NS <nameserver-name>
  Aquí, el <nameserver-name> debería ser un FQDN.

  Luego, dos nombres de servidores son listados como servidores con autoridad para el dominio.
  No es importante si estos nombres de servidores son esclavos o maestros; ambos son todavía considerados como servidores con autoridad.
  IN NS dns1.example.com. IN NS dns2.

- **PTR**

  Registro PoinTeR (puntero), diseñado para apuntar a otra parte del espacio de nombres.
  Los registros PTR son usados principalmente para la resolución inversa de nombres, pues ellos apuntan direcciones IP de vuelta a un nombre particular.

- **SOA**

  Registro de recursos Start Of Authority, que declara información importante de autoridad relacionada con espacios de nombres al servidor de nombres.
  Está situado detrás de las directivas, un registro SOA es el primer registro en un archivo de zona. El ejemplo siguiente muestra la estructura básica de un registro de recursos SOA:

```
@ IN SOA <primary-name-server> <hostmaster-email> (
                <serial-number>
                <time-to-refresh>
                <time-to-retry>
                <time-to-expire>
                <minimum-TTL> )
```

**FIGURA 4.13 Estructura del Registro de SOA**

El símbolo @ coloca la directiva $ORIGIN (o el nombre de la zona, si la directiva $ORIGIN no está configurada) como el espacio de nombres que está siendo definido por este registro de recursos SOA. El nombre del host del servidor de nombres que tiene autoridad para este dominio es la directiva
<primary-name-server> y el correo electrónico de la persona a contactar sobre este espacio de nombres es la directiva <hostmaster-email>.

La directiva <serial-number> es un valor numérico que es incrementado cada vez que se cambia el archivo de zona para así indicar a named que debería recargar esta zona. La directiva <time-to-refresh> es el valor numérico que los servidores esclavos utilizan para determinar cuánto tiempo debe esperar antes de preguntar al servidor de nombres maestro si se han realizado cambios a la zona. El valor <serial-number> es usado por los servidores esclavos para determinar si está usando datos de la zona desactualizados y si debería refrescarlos.

La directiva <time-to-retry> es un valor numérico usado por los servidores esclavos para determinar el intervalo de tiempo que tiene que esperar antes de emitir una petición de actualización de datos en caso de que el servidor de nombres maestro no responda. Si el servidor maestro no ha respondido a una petición de actualización de datos antes de que se acabe el intervalo de tiempo <time-to-expire>, los servidores esclavos

paran de responder como una autoridad por peticiones relacionadas a ese espacio de nombres.

La directiva <minimum-TTL> es la cantidad de tiempo que otros servidores de nombres guardan en caché la información de zona. Cuando se configura BIND, todos los tiempos son siempre referenciados en segundos. Sin embargo, es posible usar abreviaciones cuando se especifiquen unidades de tiempo además de segundos, tales como minutos (M), horas (H), días (D) y semanas (W).

| SEGUNDOS | TIEMPO |
|---|---|
| 60 | 1M |
| 1800 | 30M |
| 3600 | 1H |
| 10800 | 3H |
| 21600 | 6H |
| 43200 | 12H |
| 86400 | 1D |
| 259200 | 3D |
| 604800 | 1W |
| 31536000 | 365D |

**TABLA XIV UNIDADES DE TIEMPO**

A continuación detallamos la configuración de unach.edu.ec.zone

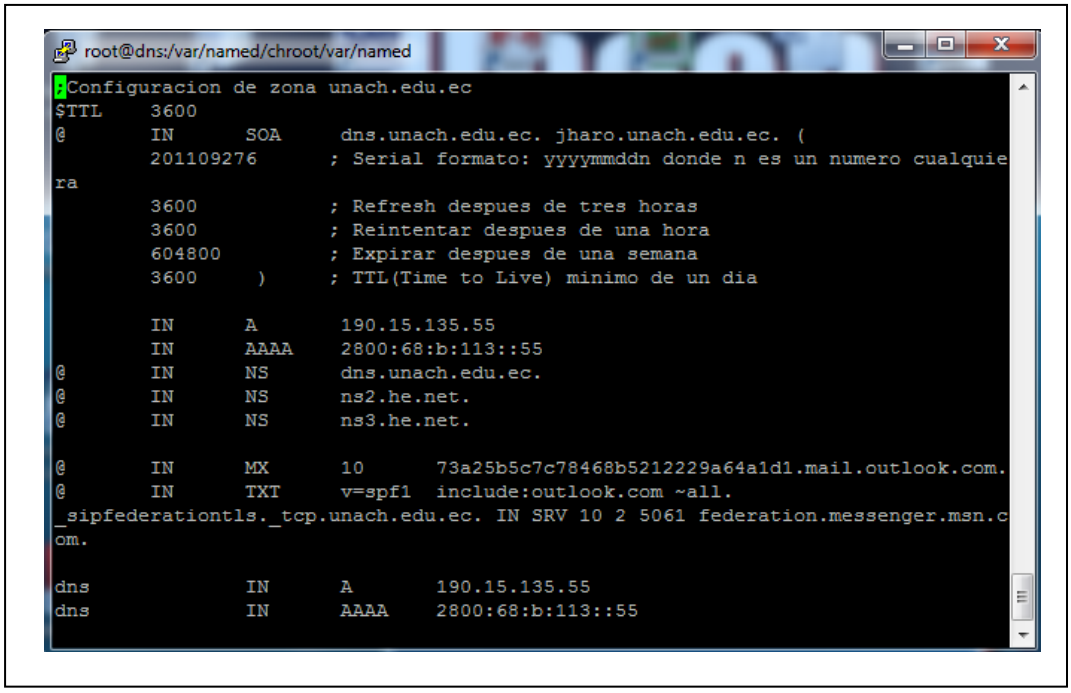



**FIGURA 4.14 /var/named/chroot/var/named/unach.edu.ec.zone**

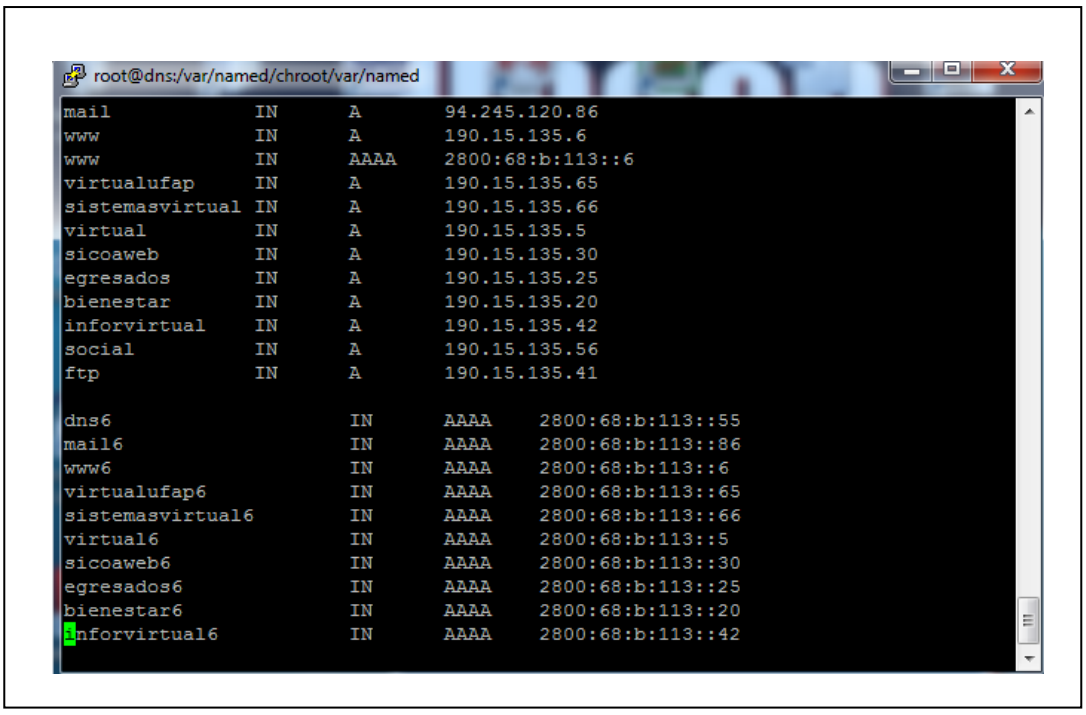



**FIGURA 4.14 /var/named/chroot/var/named/unach.edu.ec.zone**

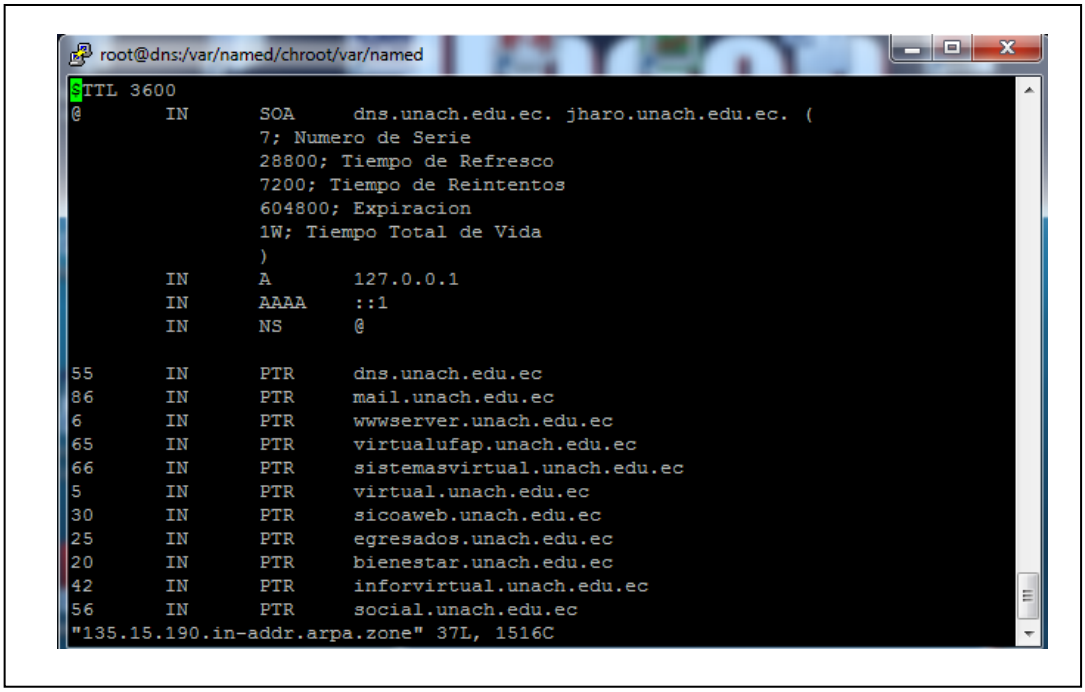



**FIGURA 4.15 /var/named/chroot/var/named/135.15.190/in-addr.arpa.zone**

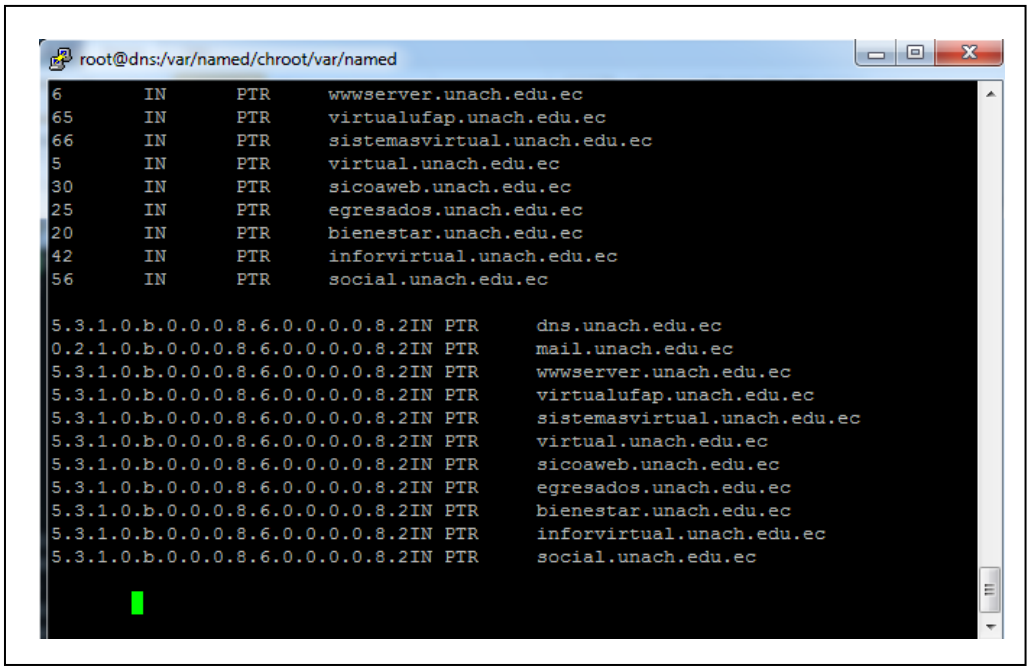



**FIGURA 4.15 /var/named/chroot/var/named/135.15.190/in-addr.arpa.zone**

También es necesario configurar el /etc/resolv.conf

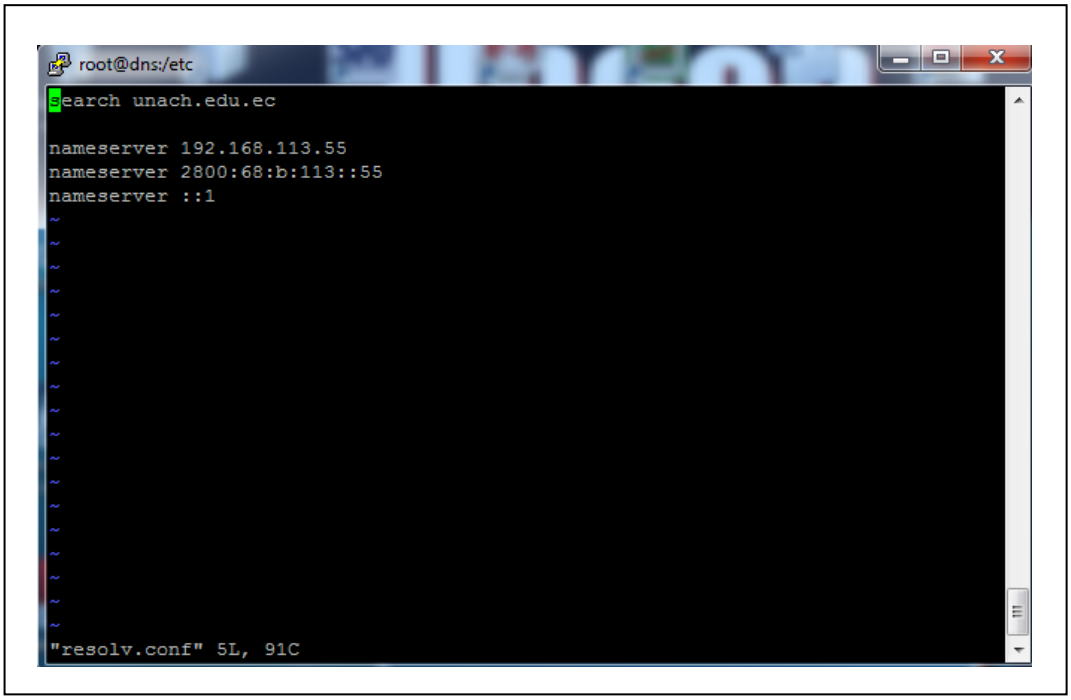



**FIGURA 4.16 /etc/resolv.conf**

La línea `search' especifica en que dominios buscar para cualquier nombre de máquina al que se desea conectar, `nameserver' especifica la dirección del servidor de nombres, en este caso el localhost, que es donde se ejecuta.

### 4.6.1.3.3 Levantar el Demonio Named del servicio DNS

Una vez configurados los archivos se debe levantar el demonio named con el comando:

service named start ó

service named reload

Para verificar que se ha levantado correctamente el servicio se puede observar el archivo

/var/log/messages, el comando sería tail –f /var/log/messages

Para que se inicie de manera automática la próxima vez que inicie el sistema, utilice lo siguiente:

chkconfig named on

### 4.6.2 SERVIDOR DE HOSTING (WEB)

Como se mencionó anteriormente el servidor WEB está en la plataforma de Windows server 2003, por lo fue necesario instalar IPv6. En realidad se diría que IPv6 ya está instalado y por tanto más que instalación hablamos de una activación.

#### 4.6.2.1 Instalación de IPv6 en el server 2003

Existen dos procedimientos para habilitar IPv6 en esta plataforma:

- **Línea de Comandos**

En una ventana DOS ejecutar:

- Ipv6 install
- Netsh interface ipv6 install

- **Interfaz gráfica**

  A través del entorno gráfico se selecciona Panel de control hasta llegar a "Conexiones de red" se selecciona "red de área local" o "red inalámbrica" se da clic derecho y se ubica con el cursor en "Propiedades" a continuación se pulsa sobre "instalar", "protocolo" y finalmente se selecciona "Microsoft TCP/IP versión 6"

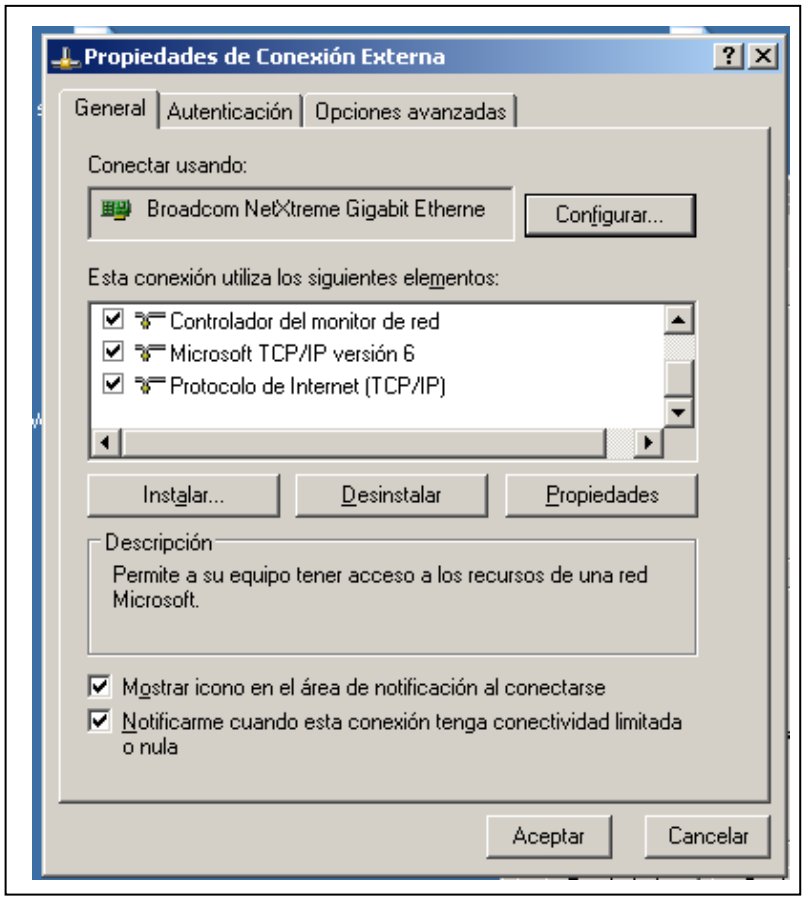



**FIGURA 4.17 PROTOCOLO IPV6 INSTALADO**

### 4.6.2.2 Configuración de una Dirección IPv6

Para asignar una dirección IPv6 y una ruta estática en el servidor web se utilizó los siguientes comandos:

- netsh interface ipv6 add address 4 2800:68:b:113::6 type=unicast validlifetime=infinite preferredlifetime=10m store=active

- netsh interface ipv6 add route 2800.68:b:113::6/ 64 ::/0 store=persistent donde ::/0 es la puerta de enlace que se configura para dicha ruta.

# CAPITULO V

# 5. PRUEBAS Y RESULTADOS

## 5.1 PRUEBAS

Una vez levantado el servicio se hará las pruebas correspondientes, con los siguientes comandos.

### 5.1.1 Nslookup (Name System Lookup)

Es una herramienta que permite consultar un servidor de nombre y obtener información relacionada con el dominio o el host y así diagnosticar los eventuales problemas de configuración que pudieran haber surgido en el DNS.


**FIGURA 5.1 PRUEBA DEL COMANDO NSLOOKUP EN EL INTERNET CON IPV6**

### 5.1.2 Dig (Domain Information Groper)

Permite realizar consultas a los servidores DNS, por lo que es muy útil para comprobar si el DNS esta correctamente configurado en nuestra maquina. Permite comprobar tanto el mapeo de nombres a IPs como el mapeo inverso de IPs a nombres, pero solo sirve para Internet, ya que no mira en  /etc/host (solo utiliza /etc/resolv.conf). Su sintaxis es:

dig [@servidor_dns] <nombre> [opciones] [tipo]

**[@servidor_dns]:** nombre o IP del servidor DNS al que queremos dirigir nuestra consulta, utilizara los servidores DNS listados en /etc/resolv.conf

**<nombre>:** nombre de dominio cuya IP queremos resolver.

**[tipo]:** tipo de consulta. Valores posibles:

**A:** IP del servidor que aloja al dominio (por defecto).

**NS:** servidores DNS.

**MX:** servidores de correo.

**ANY:** todas las anteriores.

**AAAA:** IP en IPv6.

### 5.1.3 Pruebas en Ipv4 e IPv6 de la página WEB de la UNACH

#### 5.1.3.1 Página web en IPv4: 192.168.113.6


**FIGURA 5.2 WEB IPV4**

**5.1.3.2 Página web en IPv6:** **[**2800:68:B:113::6]

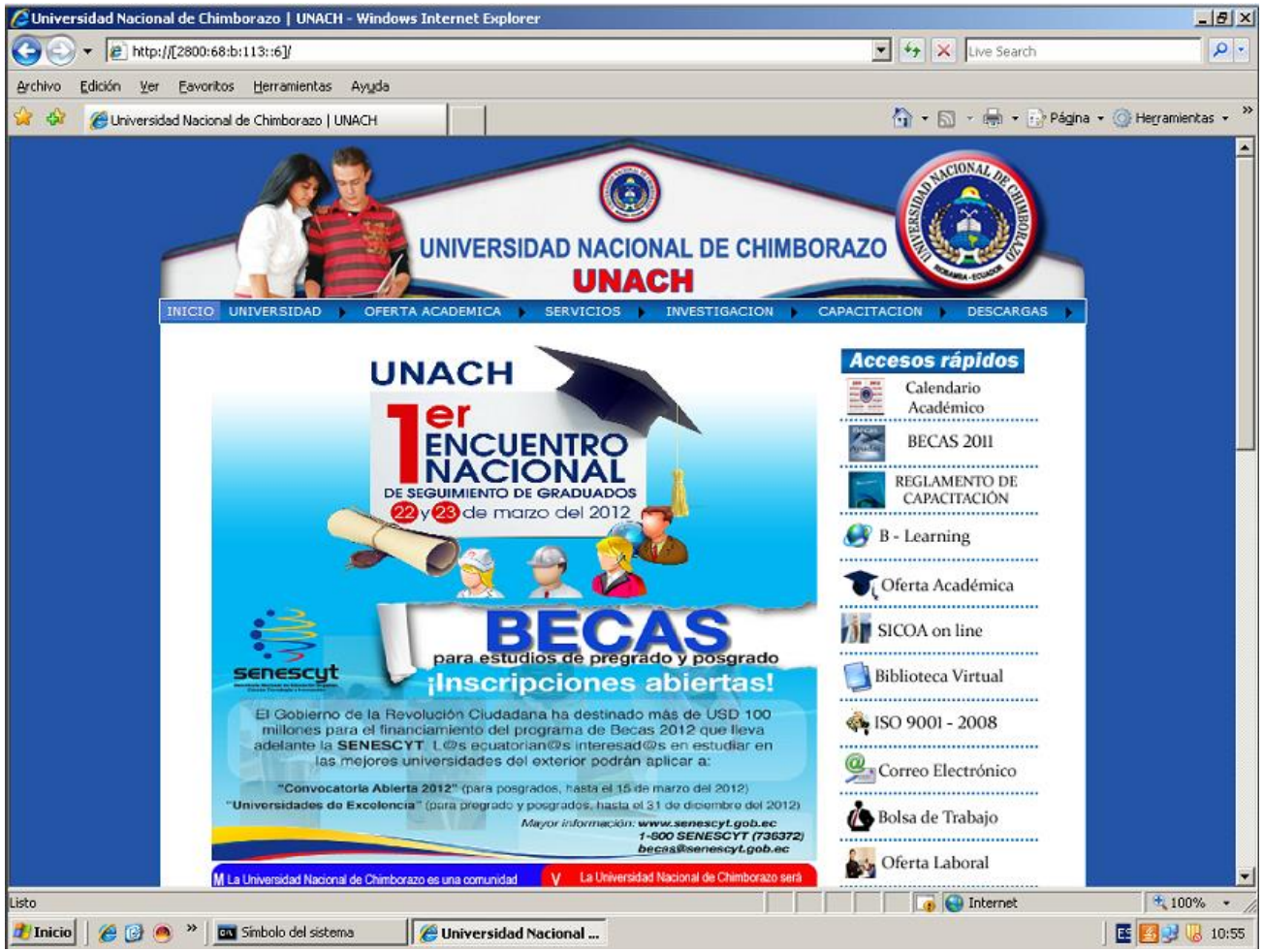



**FIGURA 5.3 WEB IPv6**

### 5.1.4 Pruebas en Ipv4 e IPv6 del Servidor DNS de la UNACH en el Internet.

#### 5.1.4.1 Página web del servidor DNS en IPv4: 192.168.113.55

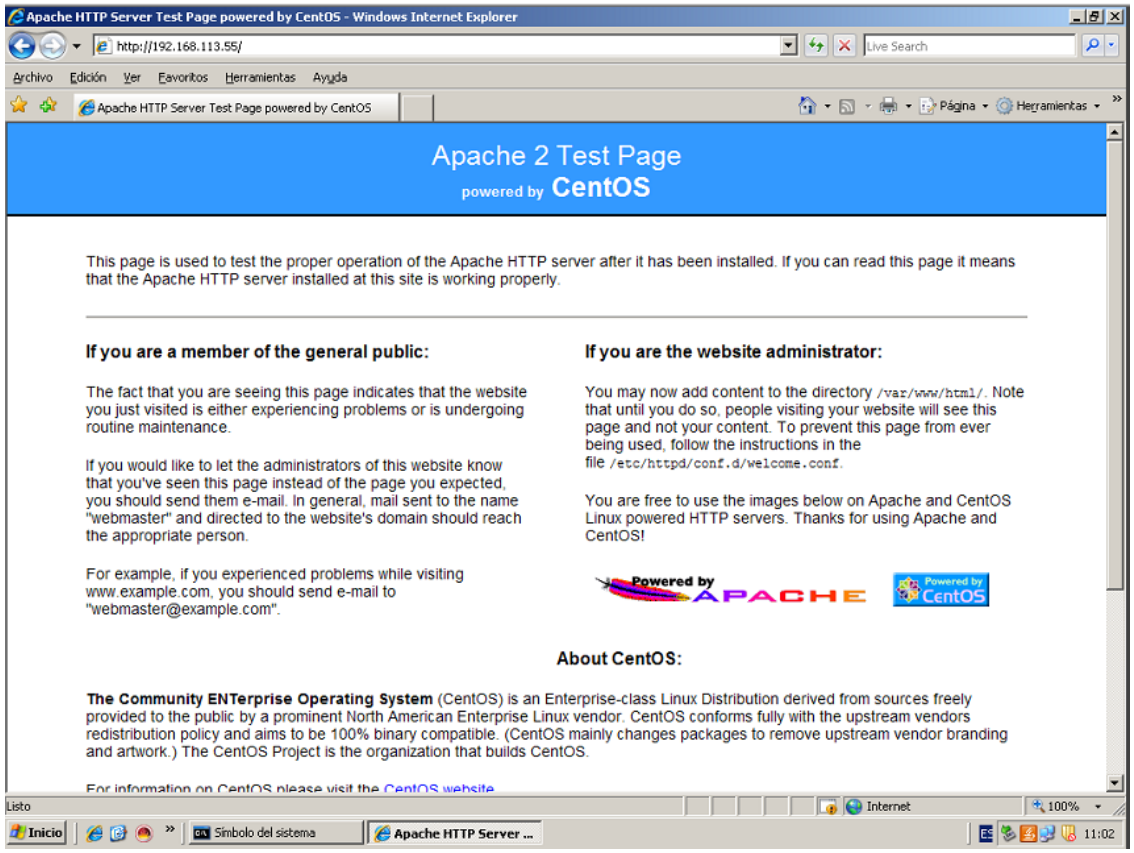



**FIGURA 5.4 DNS IPv4**

### 5.1.4.2 Página web del servidor DNS en IPv6: [2800:68:B:113::55]

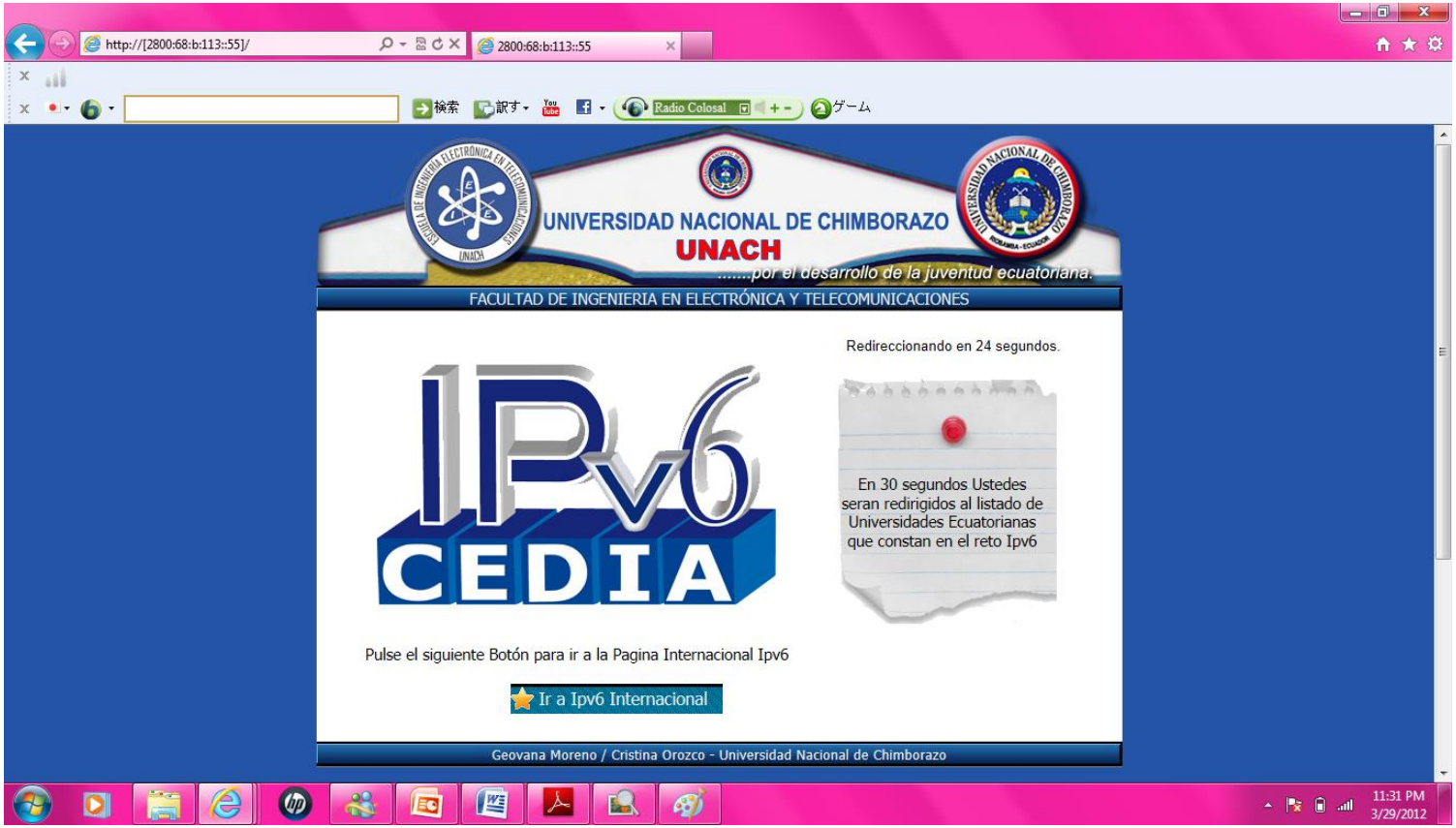



**FIGURA5.5 DNS IPv6**

### 5.1.5 Universidades que están el Reto IPv6

La siguiente pagina web es una prueba de que la Universidad Nacional de Chimborazo consta entre las 16 universidades que forman parte del reto IPv6.

El servidor DNS y WEB se encuentran en color verde, lo mismo que significa que estos servidores están funcionando correctamente.

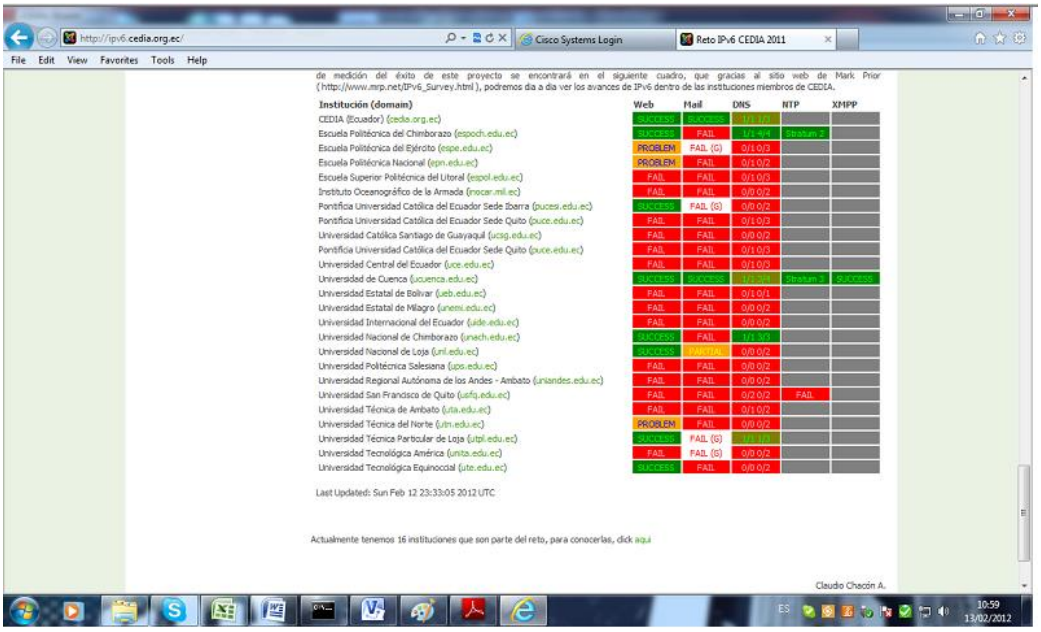



**FIGURA5.6 PAGINA WEB DE CEDIA / RETO IPv6**

### 5.1.6 Servidor WEB de la UNACH en CEDIA

A continuación podemos ver que la misma página de CEDIA nos muestra que el servidor WEB de la UNACH está en funcionamiento al corroborar que aparece la dirección IPv6 del mismo en la parte inferior.

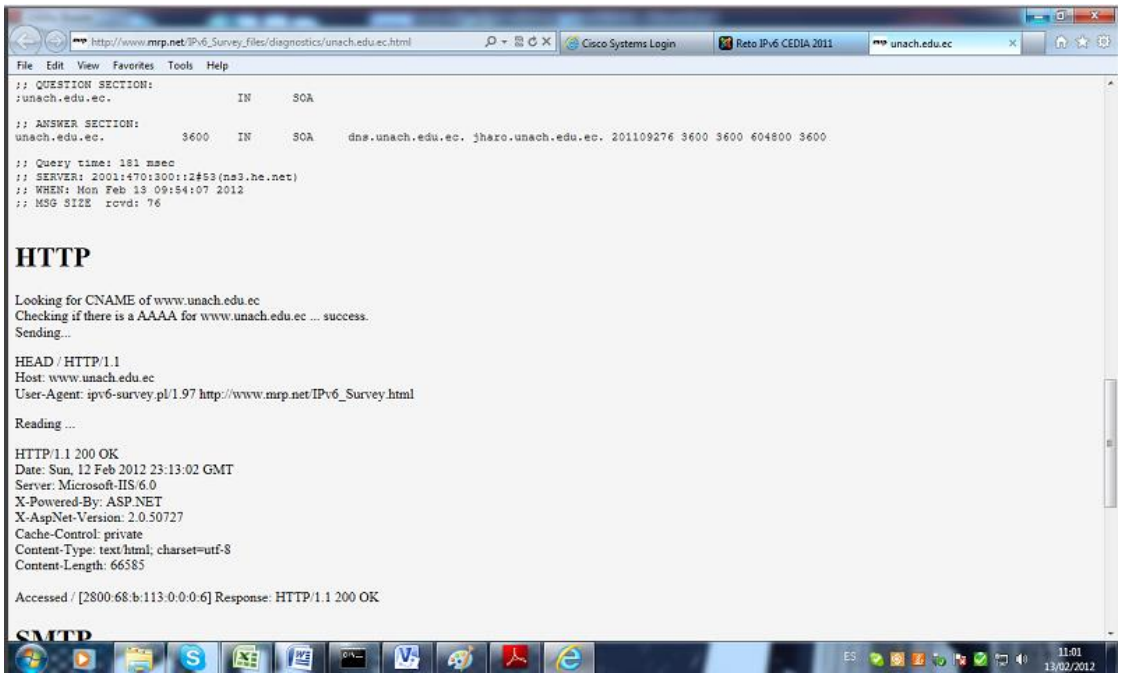



**FIGURA5.7 HTTP en CEDIA**

### 5.1.7 Servidor DNS de la UNACH en CEDIA

CEDIA nos permite constatar que el servidor DNS está levantado. Como podemos ver a, tenemos un servidor DNS maestro con la dirección IPv6 que le asignamos internamente y tenemos dos servidores DNS esclavos, los mismos que se encuentran en la nube y que entran en funcionamiento cuando el DNS maestro llega a fallar.

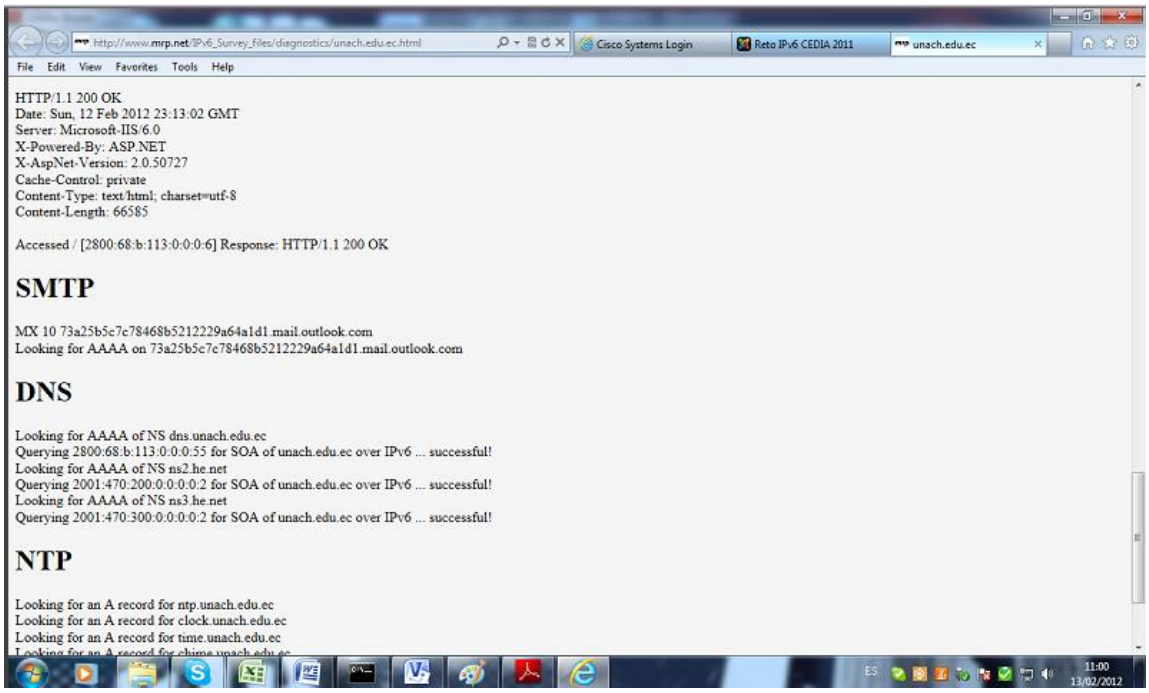



**FIGURA 5.8 DNS en CEDIA**

### 5.1.8 Pruebas con el comando ping

El comendo ping (Packet Internet Groper) sirve para saber si podemos acceder a cierta dirección IP, a cierto servidor, o incluso para comprobar si el cableado de mi red no tiene problemas de transmisión.

#### 5.1.8.1 Prueba de ping al servidor DNS

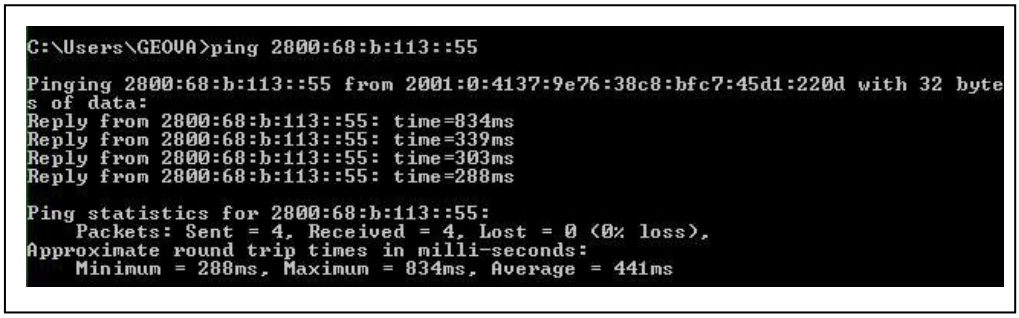



**FIGURA 5.9 PING DNS**

#### 5.1.8.2 Prueba de ping al servidor WEB

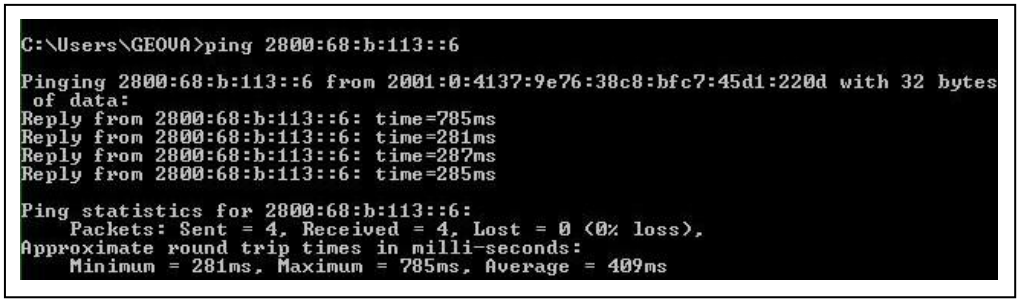



**FIGURA 5.10 PING WEB**

### 5.1.8.3 Prueba de ping a la VLAN de Administrativos

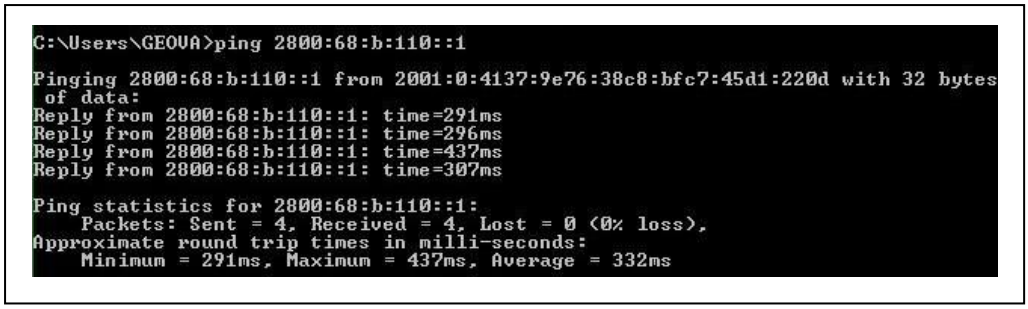



**FIGURA 5.11 PING ADMINISTRADOR**

## 5.2 RESULTADOS

Los servicios de Web, DNS están implementados con el mecanismo de transición Dual Stack (Doble Pila), lo que permitirá que los usuarios puedan acceder a los servicios de la Intranet de la Universidad Nacional de Chimborazo indiferente a la versión del protocolo IP. El impacto del protocolo IPv6 será mínima, ya que los servicios será transparentes para la los usuarios.

# CAPITULO VI

# 6.- CONCLUSIONES Y RECOMENDACIONES

## 6.1 CONCLUSIONES

- Durante el presente trabajo se diseñó e implemente una red IPv6 operando en modalidad “dual-stack” sobre la red institucional de la UNACH. La red permite conectar a las distintas unidades administrativas y departamentos directamente a Internet mediante IPv6, sin necesidad de utilizar túneles o traducción de protocolos.

- Una vez que se analizaron los servicios Web, DNS y la red interna de la Universidad Nacional de Chimborazo, se concluyó que los servicios mencionados y los dispositivos de interconexión están en la capacidad de soportar la implementación del protocolo IPv6 y a la vez coexistir con el protocolo de versión 4.

- Después de realizar la implementación en la red Institucional de la UNACH se comprobó que el tiempo de respuesta en IPv6 es mejor que en IPv4, esto se debe a que en la nueva tecnología la fragmentación se la realiza en el nodo origen y el reensamblado en los nodos finales y no en los routers como en el caso de IPv4.

- Finalmente se puede concluir que los usuarios de la Universidad Nacional de Chimborazo podrá acceder al Internet Avanzado mediante IPv4 e IPv6.

## 6.2 RECOMENDACIONES

- Es recomendable utilizar en las redes de la UNACH dispositivos y aplicaciones que estén realmente listos para trabajar tanto con IPv4 como IPv6, de tal forma que estos sean aprovechados en todo su potencial.

- Se debería realizar un plan de seguridad interno donde se definan políticas de acceso a los servidores de la UNACH, ya que en la actualidad no contamos con este servicio en la red institucional.

- Luego de la respectiva investigación se notó que existía una escases de direcciones de clase C en el protocolo de internet versión 4, por lo que se recomienda trasladarse a un direccionamiento de Clase B para contar con un rango más extenso de direcciones.

## BIBLIOGRAFÍA


- [1] TANENBAUM, Andrew S., "Redes de Computadoras", Tercera Edición, Editorial Prentice Hall Hispanoamericana S.A. México, 1997.
- [2] IPv4 Address Report. [En línea] <http://www.potaroo.net/tools/ipv4/> [consulta: 20 de Enero 2012]
- [3] Direccionamiento IPv4, Albert Nogués. [En línea] <http://albertnogues.com/attachments/014_IntroIp.pdf> [consulta 22 de Enero del 2012]
- [4] SOLENSKY, Frank. Continued Internet Growth. Proceedings of the 18th Internet Engineering Task Force. IEEE, 1990, pp 59-61.
- [5] Características del Protocolo IPv6, Felipe Ernesto Jara Saba [En línea] www.implementacionipv6.utfsm [consulta 22 de Enero del 2012]
- [6] Guía de direccionamiento, Claudio Chacón [En línea] www.cedia.org.ec [consulta 25 de Enero del 2012]
- [7]Tipos de direccionamiento Felipe Ernesto Jara Saba [En línea] www.implementacionipv6.utfsm [consulta 25 de Enero del 2012]
- [8] Mecanismos de configuración de direcciones, Mirella Rodríguez [En línea] http://repositorio.utm.edu.ec/bitstream/123456789/27/1/TESIS%20IPV6.pdf [Consulta 25 de Enero del 2012]
- [9]Protocolo Enrutado Ernesto Ariganello [En línea] http://aprenderedes.com/2006/07/protocolos-de-enrutamiento/ [consulta 25 de enero del 2012]
- [10] Protocolo de Enrutamiento, Vilma Carrillo [En línea] <http://www.slideshare.net/VILMACARRILLO/protocolos-de-enrutamiento-5139157> [consulta 2 de febrero del 2012]
- [11] Draft, Dual Stack Transition Mechanism (DSTM), Agosto 2002, J. Bound, L.Toutain, O. Medina, F. Dupont, H. Afifi, A. Durand,

<http://www.ietf.org/proceedings/02mar/l-D/draft-ietf-ngtrans-dstm-07.txt> [consulta 10 de febrero del 2012]

- [12] Direcciones y Manejos de Prefijos, Alvaro Vives [En línea] http://www.6deploy.eu/workshops2/20111010_guayaquil_ecuador/DIA1-2-PRACTICA-Direcciones-v0.1.pdf [consulta 3 de Marzo del 2012]
- [13] ACADEMIA DE NETWORKING DE CISCO SYSTEMS, Cisco "Guía del Primer Ano CCNA 1 y 2", Tercera Edición, Editorial Pearson Educacion, S.A. Madrid, 2004.

## LINKOGRAFÍA

- http://fortalezadigital08.wordpress.com/2008/09/23/protocolos-de-enrutamiento-parte-1/
- http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx
- http://www.mitecnologico.com/Main/ProtocolosDeEnrutamiento
- http://www.slideshare.net/Oscar001/clasificacion-de-los-protocolos-de-enrutamiento
- http://aprenderedes.com/2006/07/protocolos-de-enrutamiento/
- http://www.mitecnologico.com/Main/ProtocolosEnrutadosYDeEnrutamiento
- http://www.oocities.org/hilmarz/cisco/acl.htm
- http://es.m.wikipedia.org/wiki/Ping
- http://mirelucx.over-blog.com/article-29483351.html
- http://es.wikipedia.org/wiki/IPv6
- http://www.slideshare.net/zemurion/protocolos-5068655
- http://www.mitecnologico.com/Main/ProtocolosDeEnrutamiento
- http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx
- http://es.wikipedia.org/wiki/Direcci%C3%B3n_IPv6
- http://es.wikipedia.org/wiki/Direcci%C3%B3n_MAC
- http://technet.microsoft.com/es-es/library/cc736439(v=ws.10).aspx
- http://es.wikipedia.org/wiki/Tabla_de_enrutamiento

- http://www.compunauta.com/madgus/index.php/aprendiendo-linux/comandos/91-el-comando-ping-para-comprobar-una-conexion-de-red-cableado
- INTERNET SOCIETY, IPv6 Para Todos, E-Book, 2009
- DAVIES J**.,** Understanding IPV6, Washington, 2002
- http:// www.utm.edu.ec/quienes-somos/historia.asp
- http:// www.utm.edu.ec/quienes-somos/mision.asp
- es.wikipedia.org/wiki/IPv6
- www.consulintel.es/html/foroipv6/.../Tutorial%20de%20IPv6.pdf
- www.freebsd.org/doc/es_ES.../network-ipv6.html
- www.ipv6.org/
- www.cedia.org.ec/dmdocuments/17_06_05_GT_ipv6_V2.pdf
- www.consulintel.es/html/ForoIPv6/foroipv6.htm
- http://usuarios.lycos.es/janjo/janjo1.html
- http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/ipv6/ipv6.htm
- http://pdf.rincondelvago.com/transmision-de-datos_redes-ipv6.html
- http://www.ipv6ready.org