# DISEÑO E IMPLEMENTACIÓN DE LA RED Y LOS SERVICIOS INTERNET CON TECNOLOGÍA IPv6 PARA LA UNIVERSIDAD DEL CAUCA.

JENIFER QUINTERO CAMACHO
JULIÁN ANDRÉS SÁNCHEZ BARRERA

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN, 2013

# DISEÑO E IMPLEMENTACIÓN DE LA RED Y LOS SERVICIOS INTERNET CON TECNOLOGÍA IPv6 PARA LA UNIVERSIDAD DEL CAUCA

JENIFER QUINTERO CAMACHO
JULIÁN ANDRÉS SÁNCHEZ BARRERA

Trabajo de Grado presentado como requisito para optar al título de
Ingeniero en Electrónica y Telecomunicaciones

Director
Mg. Francisco Javier Terán C.

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
DEPARTAMENTO DE TELECOMUNICACIONES
POPAYÁN, 2013

**CONTENIDO**

Pág.

## LISTA DE FIGURAS

Pág.

## LISTA DE TABLAS

Pág.

# INTRODUCCIÓN

Las redes de telecomunicaciones, facilitan el transporte de datos, mejoran el uso de los recursos, disminuyen las limitaciones de tiempo y acortan distancias mediante la interconexión de los equipos, que en la actualidad no solo son estaciones fijas de trabajo, sino, también dispositivos móviles y/o inalámbricos, lo que refleja un crecimiento exponencial de la demanda de aplicaciones y servicios IP.

IPv4, es la cuarta versión del protocolo IP y la primera en ser implementada en un alto porcentaje, sobre las redes que actualmente se encuentran desplegadas, destinado a brindar $2^{32}$ direcciones lógicas en cada clase, que a principios de la década de los 80s, parecían más que suficientes, para abarcar toda la capacidad de la red global [1]; a mediados de los 90s, ya surgía una problemática relacionada con la escases de direcciones IPv4, con una incidencia mayor hoy en día, a causa de la amplia expansión de la red y los servicios soportados sobre Internet, donde las nuevas tecnologías de transmisión y de acceso se adaptaron a las telecomunicaciones, saturando la capacidad de obtener una de las cuatro mil millones de direcciones disponibles IPv4, como lo confirma la *Agencia de Asignación de Números de Internet* (*IANA*), al emitir un comunicado, afirmando que los bloques de direcciones IPv4 se han agotado. [2], [3]

De lo mencionado anteriormente, se hizo evidente un estancamiento en la prestación de los Servicios Internet y su cobertura, por esta razón, a mediados de la década de los 90s, el *Grupo de Trabajo de Ingeniería de Internet* (*IETF*), empezó a trabajar en un protocolo de la capa de red, con la intención de reemplazar paulatinamente el anterior, evitando que las redes detengan su desarrollo y crecimiento. La primera *Solicitud de Comentarios* (*RFC, Request For Coments*), de este protocolo de nueva generación *IPng*, se publicó en Enero de 1995 y se conoce como RFC 1752, donde se especifica el cambio de tamaño de las direcciones IP, y a finales del mismo año se publica la RFC 1883, la cual define los requisitos del protocolo, el formato de la PDU y señala las técnicas de direccionamiento, enrutamiento y seguridad del mismo, pero pasa a ser obsoleta en 1998, cuando es publicada la RFC 2460, el estándar actual de IPv6.[4]

Dentro de las premisas de IPv6, se encuentran métodos de migración de manera gradual, permitiendo la convivencia entre ambas versiones del protocolo, mediante tres mecanismos de transición, clasificados de acuerdo a la técnica que se utiliza:

- Túneles:
  Conectividad entre redes IPv6 a través de redes IPv4, mediante encapsulamiento de paquetes.

- Traducción:
  Comunicación entre un nodo que solo soporta IPv4, con otro que solo soporta IPv6. (Con estado – Sin estado).

- Doble Pila (*Dual Stack*):
  Implementación de ambos protocolos IP en cada nodo de la red. Esta técnica se detalla en la recomendación RFC 4213.

El interés de este trabajo, se centra en determinar una estrategia para la transición hacia IPv6, sobre la red y los servicios Internet en IPv4 de la Universidad del Cauca, ya que de acuerdo a lo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MINTIC), en la Circular 000002 del 6 de Julio de 2011-Promoción IPv6, se convoca a las entidades de la Administración Pública, Ramas y Organismos del Estado y al sector TIC, desarrollar e implementar el protocolo IPv6, sobre su plataforma y servicios prestados con compatibilidad o soporte IPv4. Además se insta, que incluyan en sus administraciones un "Plan de transición para la adopción de IPv6 en coexistencia con IPv4", que permita una transición segura y sin traumatismos para la Entidad, usuarios y para el administrador.

El desarrollo del proyecto se plasma en este documento, el cual se divide en 4 capítulos estructurados de la siguiente manera:

Capítulo 1. Plantea la estrategia utilizada para la implementación de protocolo IPv6, sobre la red y los Servicios Internet de la Universidad del Cauca.

Capítulo 2. Aplica la metodología Top-Down, para lograr establecer la red de la Universidad del Cauca, como una red Dual-Stack.

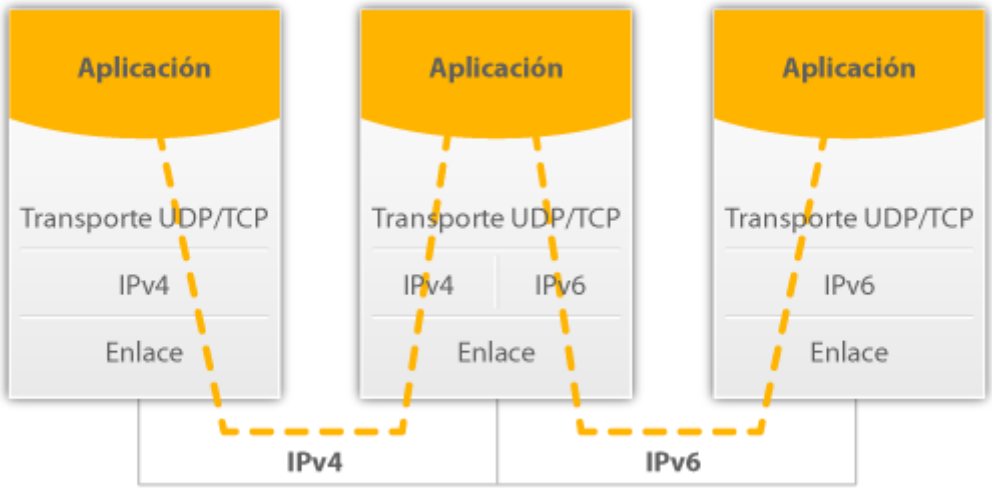
Capítulo 3. Aplica el ciclo de Deming, para la implementación de los servicios Internet de la Universidad del Cauca, con soporte IPv6.

Capítulo 4. Se exponen las conclusiones, aportes y trabajos futuros de este proyecto.

# 1 ESTRATEGIA DE TRANSICIÓN DUAL-STACK

La transición hacia IPv6, debe darse de tal manera, que no afecte la red y los servicios, que de manera inicial se tienen implementados, por tal motivo, se piensa en la implementación del protocolo IPv6, mediante la estrategia de transición Dual-Stack, la cual, consiste en implementar el nuevo protocolo, de tal manera que pueda convivir con IPv4, garantizando que, el resto de niveles en el sistema, puedan desplegarse tanto en IPv4 como en IPv6.

**Figura 1.1.1 Dual-Stack**

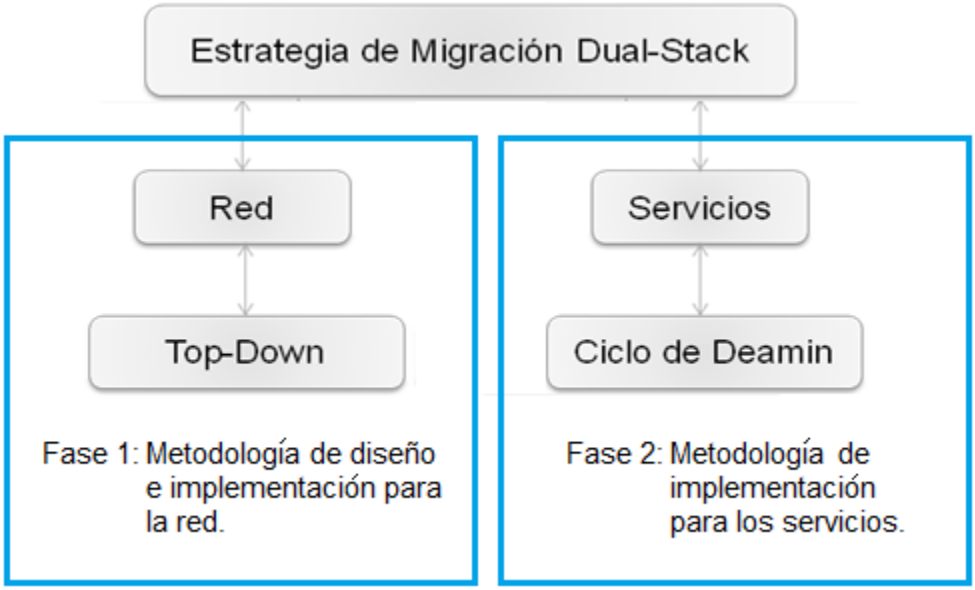



Cada nodo IPv4/IPv6, es configurado con las dos versiones de protocolo de red, con el fin de enviar y recibir datagramas que pertenecen a ambos protocolos, así como también, poder comunicar con cada nodo en la red IPv4 e IPv6. Esta es la manera más simple y más deseable para que IPv4 e IPv6 coexistan.

En este trabajo se propone una estrategia de migración hacia *Dual-Stack*, iniciando sobre la red de manera gradual, partiendo de configurar enlaces locales, para validar los impactos causados y de acuerdo a los resultados, se implementa sobre los segmentos de red menos críticos en adelante. Proceso contemplado en la metodología Top-Down, en la cual, se plantea la implementación sobre la red de manera jerárquica.

Una vez se cuenta con una red *Dual-Stack*, se procede a disponer, que los servicios Internet puedan ser accesados por nodos configurados con IPv4 y/o IPv6 y de esta manera posibilitar el acceso a los servicios, independiente del protocolo configurado en el nodo solicitante; cuya implementación se propone, mediante la metodología o ciclo de *Deamin* (*PDCA, Plan – Do – Check - Act*).

**Figura 1.1.2 Estrategia de migración. Por los autores**




En la figura 1.1.2, se observa las dos fases que componen la estrategia de migración hacia *Dual-Stack*, planteada en este documento.

## 1.1 METODOLOGÍA DE DISEÑO E IMPLEMENTACIÓN PARA LA RED

El actual estado de las redes IPv6 a nivel mundial y las recurrentes iniciativas de diferentes entes para su despliegue e implementación, han hecho que la Universidad del Cauca, mediante la división de Tecnologías de la Información y las Comunicaciones (División TIC), y la Facultad de Ingeniería Electrónica y Telecomunicaciones (FIET), decida poner a disposición de la comunidad académica: estudiantes, docentes y personal administrativo, nuevas tecnologías y servicios de red, que brinden aportes en la academia y estén dentro de los lineamientos de los objetivos de la Institución. La implementación de este nuevo protocolo, enmarcada dentro de una estrategia de migración, requiere de análisis y pruebas, que permitan establecer el alcance dentro de la Universidad del Cauca de todo el despliegue y así brindar una plataforma confiable, que soporte los Servicios Internet básicos y esté orientada a actualizaciones futuras.

Para lograr lo anterior se debe realizar un proceso de diseño y posterior implementación, acorde a las exigencias y necesidades establecidas por la administración de esta red. En la primera etapa, se hace uso de una metodología de diseño, que brinde una guía para la definición de aspectos como: análisis previo de requerimientos, limitaciones, beneficios y pruebas. Debido a que en un estado inicial, la Universidad del Cauca tiene un despliegue de equipos de red de referencia CISCO [7], para la totalidad de las tareas de enrutamiento, se toma la metodología Top-Down, como referente.

Esta metodología, se fundamenta en cuatro fases primordiales: identificación de las necesidades y objetivos del cliente, diseño de red lógico, diseño de red físico y pruebas, optimización y documentación. Todas estas abarcan exhaustivamente, pasos desde la planeación, para el despliegue de la infraestructura, análisis de viabilidad para el cliente, hasta el diseño lógico y sus pruebas y documentación como lo muestra la tabla 1.1.1.

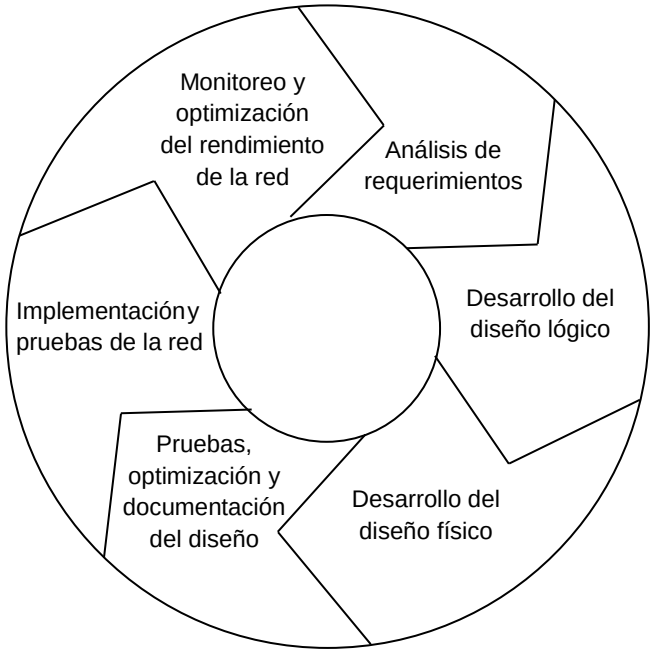
**Tabla 1.1.1 Fases metodología Top-Down**

| | |
|---|---|
| 1. | Identificación de las necesidades y objetivos del cliente |
| 1.1 | Análisis de objetivos y limitaciones del negocio |
| 1.2 | Análisis de objetivos y limitaciones técnicas |
| 1.3 | Caracterización de la red existente |
| 1.4 | Caracterización del tráfico de red |
| 2. | Diseño lógico de red |
| 2.1 | Diseño de la topología de red |
| 2.2 | Diseño de modelos para direccionamiento y denominación |
| 2.3 | Selección de protocolos de conmutación y enrutamiento |
| 2.4 | Desarrollo de estrategias de seguridad |
| 2.5 | Desarrollo de estrategias para la administración de la red |
| 3. | Diseño físico de la red |
| 3.1 | Selección de tecnologías y equipos para redes en Campus |
| 3.2 | Selección de tecnologías y equipos para redes empresariales |
| 4. | Pruebas, optimización y documentación del diseño de red |
| 4.1 | Pruebas del diseño de red |
| 4.2 | Optimización del diseño de red |
| 4.3 | Documentación del diseño |

En el diseño, para la implementación del protocolo IPv6, en la red existente y de producción de la Universidad del Cauca, se aplica selectivamente la anterior metodología, ya que en particular, se usa una infraestructura de red existente, para unos servicios limitados, lo anterior comprendido dentro de las necesidades y políticas demarcadas por la división TIC, antes del inicio del proyecto [8].

Dada la naturaleza del proyecto, que se centra en la parte lógica, relacionada con el software, la implementación se concatena, con la última fase del diseño, teniendo así unas etapas de pruebas y optimización a la par con el despliegue sobre la red, acorde al ciclo de diseño e implementación de red [9], mostrado en la figura 1.1.3. Para el final de este ciclo, se tiene entonces el protocolo IPv6 sobre la red cableada de la Institución.

**Figura 1.1.3 Ciclo de diseño e implementación de red**




Para llevar a cabo este despliegue se siguen las siguientes fases de diseño e implementación:

**Tabla 1.1.2 Fases diseño e implementación aplicadas al proyecto**

| | |
|---|---|
| 1. | Identificación de las necesidades y objetivos de la Universidad del Cauca |
| 1.1 | Análisis de objetivos y limitaciones del negocio |
| 1.2 | Análisis de objetivos y limitaciones técnicas |
| 1.3 | Caracterización de la red existente |
| 1.4 | Caracterización del tráfico de red |
| 2. | Diseño lógico de red |
| 2.1 | Diseño de la topología de red |
| 2.2 | Diseño del modelo para direccionamiento |
| 2.3 | Selección de protocolo de enrutamiento |
| 2.4 | Desarrollo de estrategias de seguridad |
| 4. | Pruebas y Optimización |
| 4.1 | Pruebas del diseño de red e implementación |
| 4.2 | Optimización del diseño de red y avances sobre la misma. |

### 1.1.1 Identificación de las necesidades y objetivos de la Universidad del Cauca

#### 1.1.1.1 Análisis de objetivos y limitaciones del negocio.

Este primer análisis, se refiere al primer contacto que se hace con la Universidad del Cauca como cliente, para así poder definir importantes aspectos para el desarrollo del proyecto, aquí se inicia con la comprensión de objetivos y filosofía, lo cual expone las metas y limitaciones precisadas por la misma o por entes de regulación.

El entendimiento de la estructura organizacional, también ayuda a reconocer la jerarquía de dirección. Uno de los primeros objetivos, en las etapas tempranas del diseño del proyecto de red, es determinar ¿quiénes son los funcionarios con poder de decisión?

Además del análisis de objetivos del negocio y determinación de la necesidad del cliente de apoyar aplicaciones nuevas, es importante analizar cualquier restricción comercial, que afecte el diseño de red y cualquier responsabilidad, que se deba asumir por algún fallo.

Hay diferentes aspectos a conocer, tales como, ¿Qué servicios se desea publicar mediante esta red?, ¿A quiénes se desea y a quiénes se puede brindar?, con esto y las anteriores aclaraciones, se logra determinar el alcance del proyecto. Para enfocarlo mejor, se hace referencia al modelo de interconexión de sistemas abiertos (*OSI, Open System Interconnection*) (ver tabla 1.1.3), el cual permite identificar las capas en las cuales se enfatiza el trabajo [10], teniendo claros los siguientes términos:

- Segmento
- LAN
- Red de edificio
- Red de campus
- WAN
- Red inalámbrica

**Tabla 1.1.3 Modelo de referencia OSI**

| |
|---|
| Aplicación |
| Presentación |
| Sesión |
| Transporte |
| Red |
| Enlace de datos |
| Física |

La tabla 1.1.4, representa una lista de verificación, la cual, determinará que la información recopilada, en conjunto con el cliente, es suficiente para definir el análisis de objetivos y limitaciones del negocio.

**Tabla 1.1.4 Lista de verificación para el análisis de objetivos y limitaciones del negocio**

| Consideración | Si | No | Observaciones |
|---|---|---|---|
| ¿Se ha investigado la industria del cliente? | | | |
| ¿Se entiende estructura corporativa del cliente? | | | |
| ¿Se ha compilado una lista de objetivos de negocio del cliente, a partir de un objetivo de negocio global que explica el propósito principal del proyecto de diseño de red? | | | |
| ¿El cliente ha identificado las operaciones críticas? | | | |
| ¿Se entiende el ámbito de aplicación del proyecto de diseño de la red? | | | |
| ¿Se ha identificado las aplicaciones de red del cliente? | | | |
| ¿El cliente ha explicado las políticas, con respecto a los proveedores autorizados, protocolos o plataformas? | | | |
| ¿Se tiene conocimiento del presupuesto para este proyecto? | | | |

### 1.1.1.2 Análisis de objetivos y limitaciones técnicas.

En esta parte, se establecen parámetros para analizar las metas técnicas de la Universidad del Cauca, con el objetivo de implementar el protocolo IPv6 en la red existente. El conocer las metas técnicas aporta a este proyecto la claridad del alcance.

Para el desarrollo de este proyecto, es importante tener en cuenta aspectos como: la escalabilidad, seguridad, usabilidad y adaptabilidad [11].

- **Escalabilidad**. Hace referencia a contemplar el crecimiento, en cuanto a usuarios, dependencias y servicios, de la red LAN de la Universidad del Cauca.
- **Seguridad**. Otro objetivo importante para la Institución, se refiere a los métodos de seguridad, aplicados tanto a la red interna como a la WAN. El diseño de red, debe garantizar la seguridad de la información de la Institución, para que no sea dañada o accedida inapropiadamente.
- **Usabilidad.** Se considera la implementación de servicios soportados en IPv6, que facilite el acceso a los usuarios finales.
- **Adaptabilidad**. Esta característica corresponde a la selección apropiada de una estrategia de migración, para la inclusión del nuevo protocolo sobre la red.

En la tabla 1.1.5, se muestra el valor asignado, de acuerdo a la prioridad que tiene cada una de las características anteriores, definidas por el administrador de redes de la Universidad del Cauca.

**Tabla 1.1.5 Prioridad de los parámetros técnicos. Por el cliente**

| Parámetro | Valor |
|---|---|
| Escalabilidad | 30 |
| Seguridad | 30 |
| Usabilidad | 10 |
| Adaptabilidad | 30 |
| **Total** | **100** |

La tabla 1.1.6, representa una lista de verificación, la cual, puede utilizarse para determinar, si se han abordado todos los objetivos y limitaciones técnicas.

**Tabla 1.1.6 Lista de verificación para el análisis de objetivos y limitaciones técnicas**

| Consideración | Si | No | Observaciones |
|---|---|---|---|
| ¿Se ha considerado los planes del cliente, para expandir el número de sitios, usuarios y servidores? | | | |
| ¿El cliente ha dicho acerca de los planes, para implementar una extranet con el fin de comunicarse con los socios u otras compañías? | | | |
| ¿Se han documentado objetivos, para el rendimiento de los dispositivos de interconexión? | | | |
| ¿Se ha hablado de los riesgos de seguridad de red y los requisitos con el cliente? | | | |
| ¿Se ha elaborado una lista de los objetivos de diseño de la red, incluyendo los objetivos y limitaciones técnicas y del cliente? | | | |

### 1.1.1.3 Caracterización de la red existente.

Una de las mejores prácticas para el desarrollo del proyecto, es la caracterización de la red existente [12], ya que esto permite ajustar aún más el alcance. Se debe conocer muy bien, la topología y estructura física, su uso y comportamiento. Se debe asegurar, ¿Qué equipos están disponibles para el despliegue de IPv6 sobre la red? y ¿cuáles necesitan actualizaciones cubiertas, por las políticas de la Institución en el numeral 1.1.1.1?

Es importante tener claridad sobre la infraestructura y el direccionamiento:

- **Caracterización de la infraestructura de red**. Es necesario, realizar varios mapas y conocer los equipos de enrutamiento y su ubicación. Esto incluye, conocer referencias y direcciones de los equipos más importantes e identificar un método para su direccionamiento y mención [13]. Se debe tener mapas de:
  - Acceso lógico a los Servicios
  - Topología lógica

- **Caracterización del direccionamiento**. Es necesario, tener en cuenta, las políticas que la Institución tiene para el direccionamiento y nombramiento, tener claro el rango de direcciones que se usa en IPv4 y las posibles limitaciones de nodos en una sub-red, si se usa resumen de rutas en equipos de capa tres y protocolos de enrutamiento.

La tabla 1.1.7, representa una lista de verificación, la cual, puede utilizarse para determinar, si se han abordado los aspectos relacionados con la caracterización de la red existente.

**Tabla 1.1.7 Lista de verificación para la caracterización de la red existente**

| Consideración | Si | No | Observaciones |
|---|---|---|---|
| ¿La topología de red y la infraestructura física, están documentados? | | | |
| ¿Las direcciones y nombres de red, se asignan de manera estructurada y están documentadas? | | | |
| ¿Se han recopilado configuraciones de dispositivos de enrutamiento y conmutación? | | | |

### 1.1.1.4 Caracterización del tráfico de red.

Dentro de las necesidades y objetivos del cliente, es necesario, identificar la caracterización del tráfico de la red[1], reconociendo las fuentes principales y destinos del mismo, así como la caracterización de la carga y comportamiento.

En esta etapa, se identifica las dependencias, que conforman la red de información de la Universidad del Cauca y la zona de aplicaciones y/o servicios Internet, consumidos por los usuarios de la misma, información que se plasmará en las tablas 1.1.8. Y 1.1.9.

**Tabla 1.1.8 Identificación de dependencias**

| Dependencia | Aplicaciones Utilizadas |
|---|---|
| | |
| | |

**Tabla 1.1.9 Identificación de los servicios**

| Servidor | Localización | Usuarios |
|---|---|---|
| | | |
| | | |

[1] Ya que el ancho de banda no se considera como obstáculo para este diseño, se omite la caracterización del tráfico, de acuerdo a lo sugerido por la metodología *Top-Down* [22].

**Tabla 1.1.10 Lista de verificación para la caracterización del tráfico de la red**

| Consideración | Si | No | Observaciones |
|---|---|---|---|
| ¿Se ha identificado las principales fuentes de tráfico y servidores? | | | |

### 1.1.2 Fase de diseño lógico

#### 1.1.2.1 Diseño de la topología de red.

Este diseño abarca la ejecución de un esquema el cual se basa en la topología lógica existente en IPv4 para reflejarla en IPv6 de manera que no implica cambios en la topología física. Esta última actúa como limitante debido a la existencia de equipos que no soporten actualizaciones o que no puedan ser reemplazados.

Se tiene en cuenta políticas de la Institución para el enrutamiento y direccionamiento, limitaciones de equipos de red para soportar el nuevo protocolo y se debe velar por mantener un esquema jerárquico basado en las capas de núcleo, distribución y acceso [14]. Para el correcto uso de dominios de colisión y de broadcast se debe hacer uso de redes de acceso local virtuales (VLAN, Virtual Local Area Network).

Como última instancia se debe tener en cuenta la seguridad, al adaptar el uso de un equipo cortafuegos para el tráfico IPv6 y que actué para todo el tráfico de la LAN y la WAN, también se debe contemplar el uso una zona desmilitarizada (DMZ, *DesMilitarized Zone*) para la ubicación de algunos servidores.

#### 1.1.2.2 Diseño del modelo para direccionamiento.

El direccionamiento es uno de los pilares para la implementación de IPv6 en la red existente de la Universidad, por lo tanto es importante hacer uso de un modelo estructurado, de lo contrario, se hace difícil la administración del enrutamiento, políticas de seguridades y asignación de direcciones. Para cumplir con los requerimientos de la Institución conviene hacer referencia al modelo usado en IPv4 y al modelo jerárquico.

En continuidad con lo anterior se define si la administración de la asignación de direcciones será centralizada para concretar qué tipo direccionamiento dinámico o estático IPv6 se va a usar, también se debe tener claridad sobre el prefijo asignado a la Universidad y los proveedores de servicio de Internet (ISP, Internet Service Provider) que soporten el protocolo.
Como buenas prácticas se deben seguir las siguientes [15]:

- Diseño de un modelo estructurado para direccionamiento antes de asignar cualquier dirección.
- Dejar espacio para el crecimiento en el modelo de direccionamiento. Si no se planea el crecimiento, más tarde se tendrá que volver a numerar muchos dispositivos.
- Asignar bloques de direcciones en una forma jerárquica para fomentar la buena escalabilidad y disponibilidad.

- Para maximizar la flexibilidad y minimizar la configuración, se debe utilizar el direccionamiento dinámico de los sistemas finales.

#### 1.1.2.3 Selección de protocolo de enrutamiento.

Este apartado ayuda a la definición de las tecnologías a usar para el enrutamiento en la capa tres del modelo OSI, y se define con los requerimientos establecidos con la Universidad en los numerales 1.1.1.1 y 1.1.1.2.

Se debe definir si se usa enrutamiento estático o dinámico. De ser estático se deben definir las rutas para cada equipo de enrutamiento ya sea de distribución, de núcleo o cortafuegos y de ser posible el enrutador de frontera. De ser dinámico se debe elegir entre los protocolos por vector-distancia y los de estado-enlace y analizar todas sus características entre ellas la distancia administrativa.

#### 1.1.2.4 Desarrollo de estrategias de seguridad.

El desarrollo de las estrategias de seguridad es una de las más difíciles tareas ya que no se debe comprometer la usabilidad y desempeño en beneficio de políticas rigurosas [16]. El despliegue de Servicios Internet que se publican a la WAN y el acceso a servicios publicados por otros es la principal causa de este enfoque; analizado desde el establecimiento de los requerimientos y limitaciones de la Institución.

Para llevar a cabo un correcto diseño de la seguridad de la red se identifican los principales nodos de la topología y las posibles políticas a aplicar en cada uno de tal manera que resguarden la información confidencial de la Institución y permitan a los usuarios el fácil acceso a los servicios internos y externos.

### 1.1.3 Pruebas y optimización

#### 1.1.3.1 Pruebas del diseño de red e implementación.

En el apartado de la pruebas del diseño se puede llegar a ser muy ambiguo dado el amplio margen para delimitarlas y realizarlas. En el caso particular de la Universidad, se debe verificar el correcto funcionamiento del direccionamiento y el enrutamiento IPv6.

Para llevar a cabo las pruebas del diseño se debe establecer un prototipo sobre el cual trabajar y del cual parta la implementación, con el área IR se define de qué manera se implementara el prototipo, si en pruebas de laboratorio, integrado en la red de producción en horas de no uso de la red o en hora con tráfico normal.

Una vez se comprueba lo anterior se procede con el despliegue sobre la red en producción mediante un plan con esquema de segmentos que va abarcando la topología desde los niveles más alejados de distribución hasta el núcleo y la WAN. Inicialmente esto se percibe como testeo pero dados los resultados puede concebirse como fases de implementación hasta completar la totalidad de los segmentos de red incluido el cortafuegos.

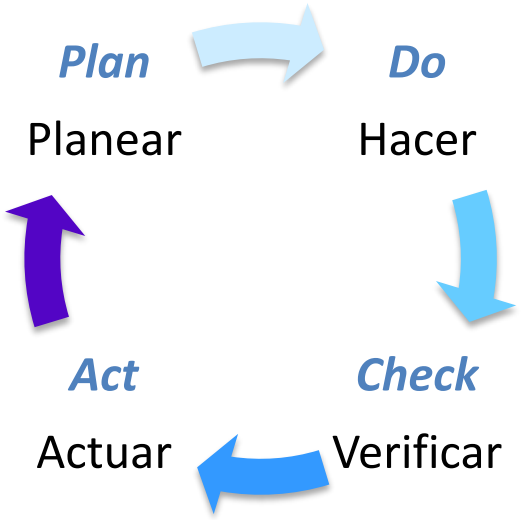
## 1.2 METODOLOGÍA DE IMPLEMENTACIÓN PARA LOS SERVICIOS INTERNET

Edward Deming dio nombre a la metodología conocida como “Ciclo de Deming” (o ciclo PDCA), aunque fue Shewhart quien realmente la desarrolló. Se trata de un ciclo de resolución de problemas y de mejora para llevar a cabo en cualquier proceso, actividad, producto o servicio.

Aplicando este concepto de PDCA a la implementación del protocolo IPv6 sobre los servicios Internet IPv4 de la Universidad se logra el mantenimiento y la mejora continua.

Este proceso consta de cuatro pasos: [5]

**Figura 1.2.1 Ciclo de Deming-PDCA**




### 1.2.1 P (*Plan*)

Establecer los objetivos y procesos necesarios para obtener los Servicios Internet de la Universidad del Cauca disponibles para ser accesados a través de redes IPv6. Esta planeación deberá comprender:

- Definir los objetivos. Se deben fijar y clarificar los límites del objetivo.
- Recopilar los datos. Se debe investigar todo el proceso actual, identificando elementos que lo componen y factores que afectarían la implementación.
- Elaborar el diagnóstico. Se deben ordenar y analizar los datos obteniendo con ello un plan de acción a seguir.
- Elaborar los pronósticos. Se deben predecir resultados frente a posibles acciones o resultados.
- Planificar los cambios. Se deben decidir, explicitar y planificar las acciones y los cambios a aplicar.

### 1.2.2 D (*Do*)

En este paso se efectúan las acciones previstas para el cambio según las decisiones y planificaciones del paso anterior, para lo cual se genera un ambiente de pruebas en el que se implantan los servicios en cuestión y de esta forma hacer ensayos y ajustes hasta conseguir una implementación eficaz y simple de mantener aplicable sobre el ambiente real, realizando modificaciones en pequeña escala, es decir, modificando aspectos sencillos y que no sean críticos. De esta forma, se tiene la posibilidad de revisar las acciones y modificar aquellos puntos que así lo requieran.

Una vez comprobada la validez del modelo sobre el ambiente de pruebas, se puede proceder a su implantación real, llevando las acciones planificadas a todo el proceso.

Acciones genéricas que incluye este paso:

- Formación del personal que deba aplicar las soluciones propuestas.
- Verificación de las acciones correctivas definidas en el plan.
- Introducción de modificaciones de no haberse obtenido resultados positivos de las medidas correctivas.
- Documentación del trabajo desarrollado y de los resultados obtenidos.

### 1.2.3 C (Check)

Una vez llevados a cabo todos aquellos cambios planificados en el proceso, se debe realizar una verificación de los mismos y comprobar los resultados obtenidos comparándolos con los previstos y especificaciones iniciales, para evaluar si la implementación del protocolo IPv6 sobre los servicios se dio de manera apropiada.

Acciones genéricas que incluye este paso:

- Verificar el correcto funcionamiento de los servicios implementados.
- Comprobar resultados obtenidos con las especificaciones iniciales.
- Identificación de no conformidades.
- Establecimiento de acciones correctivas y preventivas.

### 1.2.4 A (Act)

El Actuar son todas aquellas modificaciones que se tengan que realizar para corregir las fallas detectadas en el paso anterior. Mientras se cambien todos los aspectos necesarios, se irán comprobando y comparando con el objetivo final del proceso, de modo que al final del mismo, se tengan ejecutados todos los cambios previstos.

Acciones genéricas que incluye este paso:

- Modificar los procesos según las conclusiones del paso anterior para alcanzar los objetivos con las especificaciones iniciales, si fuese necesario.
- Aplicar nuevas mejoras, si se han detectado en el paso anterior.
- Documentar el proceso.

En resumen, el ciclo PDCA es una importante herramienta de gestión la cual se utiliza en este trabajo para llevar a cabo la implementación de los servicios Internet IPv6 permitiendo las mejoras continuas de acuerdo a los resultados de cada una de sus etapas.

# 2 DISEÑO E IMPLEMENTACIÓN DE LA RED IPv6

Como primera etapa para la consecución de una red IPv6 desplegada sobre la infraestructura existente, se sigue la metodología *Top-Down*, adaptada a la Universidad del Cauca, definida en el capítulo anterior. Dada la naturaleza de la Institución de carácter académico y no de prestación de Servicios comerciales de red e Internet, el desarrollo del proyecto se debe realizar directamente, bajo el apoyo de la División de las Tecnologías de la información y las Comunicaciones (TIC). Por lo anterior cuando se hace mención al cliente se refiere a esta dependencia.

Las áreas de Infraestructura de Red (IR) y Servidores Servicios Internet (SSI), se ven comprometidas con esta implementación, debido a la responsabilidad en la administración de la red y los servicios respectivamente.

Con respecto a lo anterior, se enumeran las siguientes fases:

## 2.1 IDENTIFICACIÓN DE LAS NECESIDADES Y OBJETIVOS DE LA UNIVERSIDAD DEL CAUCA

Para establecer el alcance del proyecto se definieron muy bien con la División TIC los requerimientos y limitaciones que se tienen para el acceso a la información, a la red, y configuraciones que permitan en un tiempo limitado desplegar el protocolo.

### 2.1.1 Análisis de objetivos y limitaciones de la Universidad del Cauca

La División TIC dentro de su misión de brindar soluciones tecnológicas, acorde a las necesidades de usuarios académicos y administrativos [17], se asegura de mantener una red LAN accesible con disposición de servicios como el correo electrónico, servicios de transferencia de archivos (*FTP, File Transfer Protocol*), servicios de videoconferencia y portales WEB. El acceso a esta red y servicios debe ser constante y lo más sencillo posible.

**Tabla 2.1.1 Identificación de usuarios y servicios de la red de información de la Universidad del Cauca**

| Usuarios de la red de la Universidad del Cauca | Servicios Internet utilizados |
|---|---|
| Academia | Correo Electrónico<br>FTP<br>WEB<br>Video conferencia |
| Administrativos | |

En este apartado se establecen con el área de infraestructura, los objetivos que tiene con la prestación de los servicios a la comunidad universitaria, los cuales exigen cierto nivel de discreción en la administración. Así, se aclara que el diseño de la topología, el direccionamiento y el enrutamiento, debe ser aprobado por esta área. También se establece que en la etapa de implementación, es el personal administrativo de la red y los servicios, quien debe hacer las configuraciones de los equipos de red de acuerdo a un plan de implementación a desarrollar con el área.

Otro ámbito de trabajo se da con el área SSI, la cual se encarga de la administración del cortafuegos. Se definió que el jefe de área es quien aprueba las políticas que se deben implementar en este y que estas serán configuradas por él.

**Tabla 2.1.2 Identificación de las áreas que conforman la división TIC y su responsabilidad frente a este proyecto**

| Áreas de la división TIC | Administrador | Responsabilidad |
|---|---|---|
| IR | Ing. Jaime Martínez<br><br>Ing. Andrés Zúñiga | Aprobación del diseño topológico de direccionamiento y enrutamiento propuesto.<br><br>Configuración de los equipos de red. |
| SSI | Ing. Fabián Mera | Configuración de las directrices, para habilitar el soporte IPv6, sobre los servicios Internet.<br><br>Aprobación de las políticas de seguridad sobre el cortafuegos. |

Para enfocar correctamente el desarrollo del proyecto se aclara que este solo se ve afectado por las capas de red, transporte y aplicación, por lo cual se excluye el análisis y modificaciones físicas.

Debido a la criticidad de la información que se transporta en el segmento denominado Financiera, el área aclara que este no hace parte del alcance del proyecto.

Finalmente se determina que para la configuración del acceso a la WAN, los integrantes de este proyecto son quienes deben contactar al ISP que tenga adelantos en IPv6, en un principio se planeó con *Telefonica*, sin embargo, debido a cambio de proveedores por parte de la Institución para el año 2012, se debe contactar con EMTEL desde enero de este año.

Los anteriores requerimientos y limitaciones por parte del cliente se establecen en un límite de tiempo de nueve meses acorde al desarrollo del proyecto de grado.

A continuación se elabora la lista de verificación para el análisis de objetivos y limitaciones del negocio.

**Tabla 2.1.3 Lista de verificación para el análisis de objetivos y limitaciones del negocio**

| Consideración | Si | No | Observaciones |
|---|---|---|---|
| ¿Se ha investigado la industria del cliente? | X | | Se considera la red de la Universidad del Cauca como académica, con prestación de servicios a usuarios administrativos y estudiantes. |
| ¿Se entiende estructura corporativa del cliente? | X | | Se identifican las áreas de la división TIC de la Universidad del Cauca involucradas para el desarrollo de este proyecto: IR y SSI. |
| ¿Se ha compilado una lista de objetivos de negocio del cliente, a partir de un objetivo de negocio global que explica el propósito principal del proyecto de diseño de red? | X | | Se define que la implementación del protocolo IPv6, no se aplicara sobre la dependencia financiera de la Universidad del Cauca, dada la criticidad de la información manejada. |
| ¿El cliente ha identificado las operaciones críticas? | X | | El diseño topológico de direccionamiento y enrutamiento, y definición de políticas en el cortafuegos, deben ser aprobados antes de ser implementados sobre la red. |
| ¿Se entiende el ámbito de aplicación del proyecto de diseño de la red? | X | | La red de información de la Universidad del Cauca, hace referencia a la LAN cableada, mas no a las dependencias a las cuales el ISP, brinda conexión. |
| ¿Se ha identificado las aplicaciones de red del cliente? | X | | Correo Electrónico<br>FTP<br>WEB<br>Video conferencia |
| ¿El cliente ha explicado las políticas, con respecto a los proveedores autorizados, protocolos o plataformas? | X | | Se identifica el ISP, con el que se configurará el acceso a la WAN IPv6. Se define el enlace WAN IPv6, hacia RENATA. |
| ¿Se tiene conocimiento del presupuesto para este proyecto? | X | | Se establece que la implementación del protocolo, se hará, sobre los equipos que lo soporte o cuya actualización no considere una inversión económica. |

### 2.1.2 Análisis de objetivos y limitaciones técnicas

Después de definir el alcance basado en políticas administrativas de la Institución, se aclara con las áreas comprometidas, que al final del despliegue, se debe tener la red IPv4 existente, sin verse afectada junto a la red IPv6, operando en los equipos de red que soporten el protocolo o permitan actualizaciones que no incurran en costos económicos. Esta red debe estar disponible para los usuarios de manera transparente, sin afectar el uso ordinario.

El área de IR, define por políticas internas, con el objetivo de mantener bajo el procesamiento en los dispositivos, hacer uso de rutas estáticas en el apartado de enrutamiento, esto en simetría con la red IPv4. Adicional a esto, la configuración existente de *dual-homing*[2], no se puede mantener en IPv6, debido a limitaciones técnicas y contractuales del proveedor ETB, tampoco se planea alcanzar las sedes remotas, debido a la intervención del proveedor en el proceso [7], lo cual no está dentro del alcance de la Universidad. Respecto a este tema se tiene una limitación para el alcance de Internet debido a que el prefijo asignado por la Red Nacional Académica de Tecnología Avanzada (RENATA) solo puede ser enrutado hacia esta red contemplada como WAN.

La red inalámbrica debe ser excluida del proyecto debido a limitaciones software del controlador el cual no garantiza la funcionalidad de asignación de direcciones, enrutamiento y administración del protocolo, en el mismo sentido si puede afectar el uso de la red existente.

De acuerdo con la metodología *Top-Down* se encuentra que la red de la Institución está basada en un nivel jerárquico, por lo tanto el diseño se debe ceñir al uso de VLANs, capa de acceso, distribución y núcleo.

Con el área SSI se estableció que la Universidad cuenta con dos equipos cortafuegos, sin embargo solo se puede operar uno en IPv6 debido a limitaciones hardware y software.

[2] Dual-homming. Hace referencia a dispositivos con dos conexiones de red, en particular para la Universidad del Cauca se refiere a la disposición de los ISPs

**Tabla 2.1.4 Limitaciones técnicas para el despliegue del protocolo IPv6 sobre la red de información de la Universidad del Cauca**

| Limitantes | Justificación |
|---|---|
| Uso exclusivo de enrutamiento IPv6 estático. | La implementación de protocolos de enrutamiento dinámico, sobre IPv6, aumentaría el procesamiento de los dispositivos. |
| No soporte de *Dual-Homing* sobre IPv6 | El proveedor ETB, presenta limitaciones técnicas frente al protocolo IPv6. |
| Alcance de redes IPv6 no pertenecientes a redes académicas. | Dependencia del soporte IPv6, sobre los equipos de red de los proveedores.<br>El prefijo IPv6 de la Universidad del Cauca, fue asignado por RENATA. |
| Red inalámbrica | Limitaciones del software del controlador inalámbrico. |
| Cortafuegos | Limitaciones de hardware y software en uno de los dos cortafuegos disponibles en la red de la Universidad del Cauca. |

- **Escalabilidad**. En la sección 2.2.2, se considera un modelo de direccionamiento flexible al crecimiento, basado en una estructura jerárquica para los nodos de la red.
- **Seguridad**. Se propone la implementación de reglas de filtrado de trafico IPv6, sobre el cortafuegos.
- **Usabilidad**. Se implementan los servicios DNS y DHCP, soportados en versión 6, sobre la red *Dual-Stack*, para así facilitar la configuración de la red y acceso a los usuarios finales.
- **Adaptabilidad**. Se establece *Dual-Stack*, como estrategia de migración y de esta manera garantizar el soporte de la red y los servicios sobre IPv4 y/o IPv6.
  Se define que la implementación se aplicara de manera gradual, empezando por los segmentos que los administradores consideran como menos críticos, de acuerdo, a la cantidad de tráfico.

**Tabla 2.1.5 Lista de verificación para el análisis de objetivos y limitaciones técnicas**

| Consideración | Si | No | Observaciones |
|---|---|---|---|
| ¿Se ha considerado los planes del cliente, para expandir el número de sitios, usuarios y servidores? | X | | Se considera un modelo de direccionamiento IPv6 jerárquico y flexible al crecimiento. |

| | | | |
|---|---|---|---|
| ¿El cliente ha dicho acerca de los planes, para implementar una extranet para comunicarse con los socios u otras compañías? | X | | Se considera la implementación del protocolo IPv6 sobre el enlace WAN, hacia RENATA, con el fin de elaboración de trabajos académicos futuros. |
| ¿Se han documentado objetivos, para el rendimiento de los dispositivos de interconexión? | X | | Se define la implementación de protocolos de enrutamiento IPv6 estático, con el fin de mantener la estabilidad en el procesamiento de los dispositivos de red. |
| ¿Se ha hablado de los riesgos de seguridad de red y los requisitos con el cliente? | X | | Se considera la implementación de reglas de filtrado para el tráfico IPv6 sobre el cortafuegos. |
| ¿Se ha elaborado una lista de los objetivos de diseño de la red, incluyendo los objetivos y limitaciones técnicas y del cliente? | X | | En la Tabla 2.1.4, se identifican las limitaciones técnicas para el despliegue del protocolo IPv6 sobre la red de información de la Universidad del Cauca. |

### 2.1.3 Caracterización de la red existente

- **Identificación de la topología de red y estructura física:**

La red de información institucional está constituida por una Red de Área Local (LAN, Local Area Network), con transmisión sobre redes Giga Ethernet en cable de Par Trenzado no Blindado (UTP, *Unshielded Twisted Pair*) y fibra óptica, como lo definen los estándares 802.3ab y 802.3z del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, *Institute of Electrical and Electronics Engineers*).

La topología de red está ligada a la estructura física que se divide en los sectores de: Ciencias Contables, Educación, División Financiera, El Carmen, Ingenierías, IPET, Medicina, Santo Domingo, Sistemas y Vicerrectoría de Investigaciones. Esta es una topología de doble estrella con centro en los edificios del Instituto de Posgrados en Ingeniería Electrónica y Telecomunicaciones (IPET) y el Carmen, en la cual el Proveedor de Servicios de Internet (ISP, *Internet Service Provider*), interviene para la conexión a la intranet de las sedes remotas, a las que la Universidad presta el servicio, como la Facultad de Ciencias Agropecuarias en la sede de las Guacas, Consultorio Jurídico, Centro de salud Alfonso López y Santander de Quilichao [7], como se ilustra en la figura 2.1.1. y se resume en la tabla 2.1.6.

**Figura 2.1.1 Topología de red IPv4**

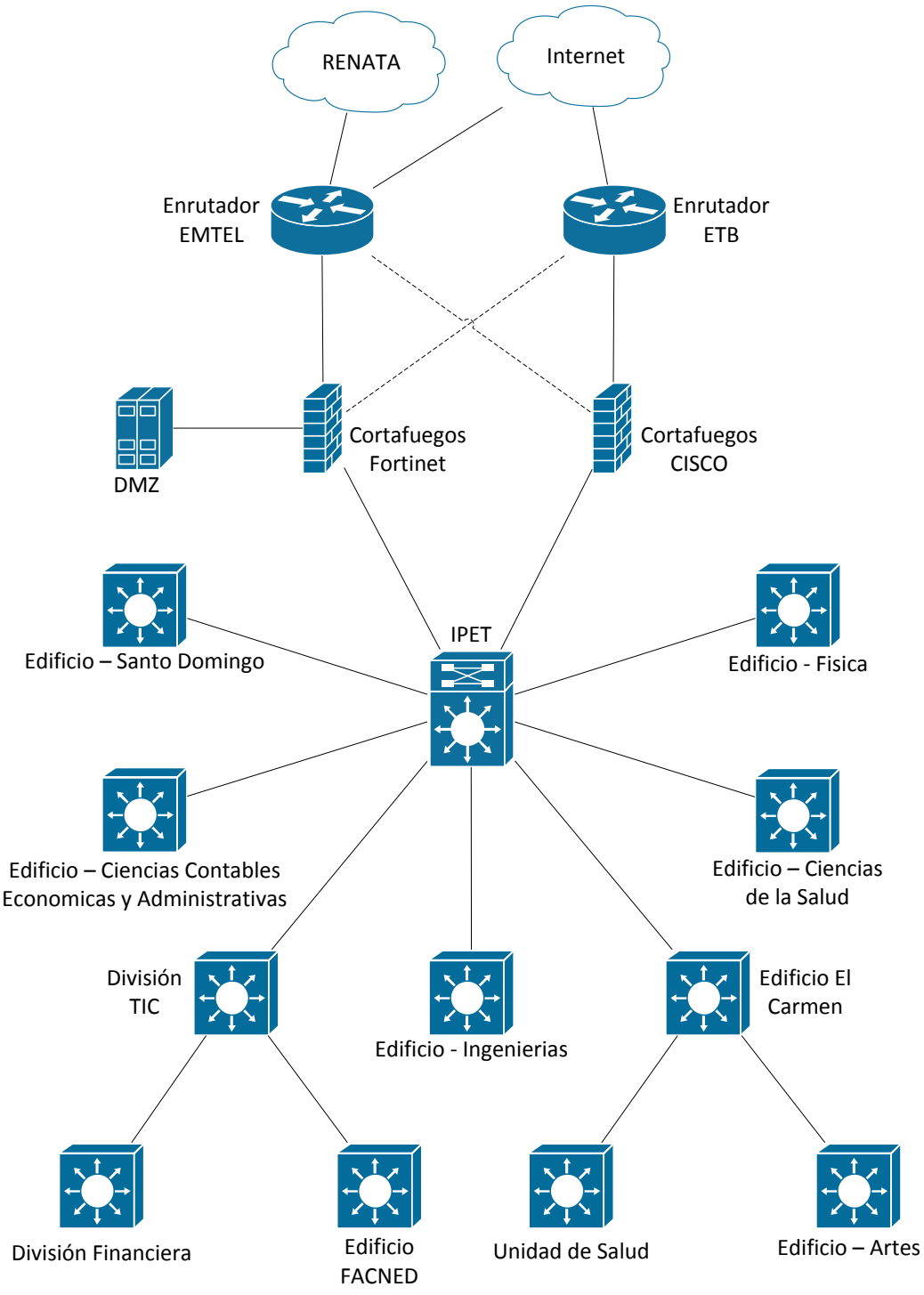


**Tabla 2.1.6 Dependencias / Nodos de red de información de la Universidad del Cauca**

| Dependencia/Nodo de Red | Interconexión |
|---|---|
| Ciencias contables | Directa |
| Educación | Directa |
| División financiera | Directa |
| El Carmen | Directa |
| Ingenieras | Directa |
| IPET | Directa |
| Medicina | Directa |
| Santo Domingo | Directa |
| Sistemas | Directa |
| Vicerrectoría de investigaciones | Directa |
| Facultad de Ciencias Agropecuarias | A través del ISP |
| Consultorio jurídico | A través del ISP |
| Centro de Salud Alfonso López | A través del ISP |
| Santander de Quilichao | A través del ISP |

- **Identificación de equipos disponibles para el despliegue de IPv6:**

La infraestructura de red de la Institución tiene un diseño jerárquico, con capas bien definidas, como lo son el núcleo, distribución y acceso desplegado con equipos de referencia CISCO, para los dos niveles superiores y para el tercer nivel, en su mayoría, de la misma marca con algunos dispositivos 3COM y Nortel que están siendo reemplazados paulatinamente por la referencia predominante.

Dado el enfoque del proyecto, es de primordial importancia el estado de las capas con funciones de enrutamiento, como el conmutador Cisco Catalyst 6509, que actúa como núcleo de la red y está ubicado en el edificio del IPET, que es el punto más importante de la red, como lo muestra la figura 2.1.1. Físicamente a este equipo llega todo el tráfico de la LAN y mediante rutas estáticas, es el encargado de dar acceso a los servicios de la Institución y a la Red de Área Amplia (WAN, *Wide Area Network*). Para el nivel de distribución se usan conmutadores Cisco de la serie Catalyst 3750; once equipos capa 3 de acuerdo al modelo de referencia OSI ubicados individualmente en cada uno de los edificios mostrados anteriormente. En el nivel de acceso predominan los conmutadores Cisco de la serie Catalyst 2960 los cuales se usan básicamente para aumentar el número de host; no se profundiza en su configuración debido a que no compete a los objetivos del proyecto. Esta información se resume en la tabla 2.1.7.

**Tabla 2.1.7 Equipos de núcleo, distribución y acceso de la red de información de la Universidad del Cauca**

| Equipo | Nivel | Versión IOS[3] | Cantidad |
|---|---|---|---|
| CISCO Catalyst 6509 | Núcleo | 12.2 (53) | 1 |
| CISCO Catalyst 3750 | Distribución | 12.2 (53) | 11 |
| CISCO Catalyst 2960 | Acceso | 12.2 (53) | 40 |

Los once equipos de distribución CISCO Catalyst 3750, están configurados con diez VLANs, que separan el tráfico de: estudiantes, docentes, administrativos, red inalámbrica, videoconferencias, servidores, sistemas de información, cámaras, VoIP y biométricas, para cada una de las dependencias o facultades de la Universidad. La aplicación de estas VLANs, complementa el fundamento del diseño jerárquico, en la medida que permite, aislar tráfico de nivel 2, ya que de no hacerse una correcta segmentación de red, se generarían retardos sobre ella. Estos equipos, enrutan todo el tráfico en dirección al CORE, haciendo uso de rutas estáticas, lo cual favorece el procesamiento en ellos y el trafico enrutado. En estos equipos no se implementan Listas de Control de Acceso (ACL, *Access Control List*), para el tráfico de los clientes, llevando a que la configuración de estos no sea demasiado compleja. Cuenta con una configuración de direccionamiento y de establecimiento de los agentes de retransmisión para el Protocolo de Configuración Dinámica de Host (DHCP, *Dynamic Host Configuration Protocol*). Esta información se resume en la tabla 2.1.8.

**Tabla 2.1.8 Configuraciones generales sobre equipos CISCO Catalyst 3750**

| | |
|---|---|
| **Configuraciones generales CISCO Catalyst 3750** | VLANs:<br>1. Estudiantes.<br>2. Docentes.<br>3. Administrativos.<br>4. Inalámbrica.<br>5. Videoconferencia.<br>6. Servidores.<br>7. Sistemas de información.<br>8. Cámaras.<br>9. VoIP.<br>10. Biométricas. |
| | Direccionamiento estático. |
| | Sin políticas de ACL. |
| | Configuración de agentes de retransmisión para el control del DHCP. |

[3] Desde la versión de IOS 12.2(2) de CISCO, se soporta el protocolo IPv6. [23]

- **Identificación del direccionamiento IPv4 en uso de la Universidad del Cauca.**

Para dar cobertura a toda la red y servicios, el direccionamiento IPv4 en uso de la Universidad del Cauca, cubre los tres tipos de direcciones privadas, distribuyéndolas, como se indica en la tabla 2.1.9.

**Tabla 2.1.9 Direccionamiento IPv4 de la red de información de la Universidad del Cauca**

| Red | Asignación |
|---|---|
| 192.168.0.0/16 | LAN |
| 10.0.0.0/8 | Servidores y red inalámbrica |
| 172.16.0.0/12 | Algunos servidores |

- **Identificación de enlaces WAN:**

Una situación crítica, para la consecución del proyecto fue, que los ISPs iniciales, ETB y Telefónica, no tienen configurado IPv6 sobre los enrutadores de frontera, ubicados en la Universidad del Cauca, sin embargo, el segundo es el proveedor oficial de RENATA, por lo cual no tiene inconvenientes en dar salida a Internet 2 con el nuevo protocolo, pero en Diciembre de 2011, la Universidad licitó para estos contratos, y los ISPs seleccionados fueron EMTEL y ETB, dentro de las exigencias del contrato, la Universidad solicitó el soporte IPv6, para la conexión a las redes académicas.

Actualmente se cuentan con dos enlaces WAN: uno en EMTEL, el cual ofrece 90 Mbps de ancho de banda de conexión, este brinda el enrutamiento hacia las redes Internet comercial e Internet 2, el otro enlace está a cargo de ETB que brinda 60 Mbps de velocidad, este proveedor no brinda conexión a las redes académicas. Cada uno de estos canales tiene a cargo un tráfico especifico, el primero, brinda la navegación para usuarios que hacen uso de NAT, como también, es el que brinda la salida a Internet para los servicios institucionales como correo electrónico, servicios WEB y FTP, el segundo se usa para la navegación de los servidores proxy. Esta información se resume en la tabla 2.1.10.

**Tabla 2.1.10 Comparación de características de los enlaces WAN de la Universidad del Cauca**

| EMTEL | ETB |
|---|---|
| Ancho de banda: 90 Mbps | Ancho de banda: 60 Mbps |
| Salida a Internet comercial y académico | Salida a Internet comercial |
| Salida de usuarios, a Internet comercial, a través de NAT | Salida de servidores proxy a Internet comercial |
| Salida a Internet para los servicios institucionales (Correo, WEB, FTP) | |

- **Identificación de componentes capa 3 para la implementación del protocolo IPv6:**

Para conocer el estado inicial de la red de la institución en la implementación de IPv6, se deben tener en cuenta algunos aspectos técnicos:

La infraestructura de la red se encuentra en buena disposición, al momento de iniciar la implantación del protocolo, esto debido a que el CISCO IOS, ha sido actualizado a la versión 12.2 (53), para todos los componentes de la red de la referencia mencionada. Los equipos de mayor beneficio con esto son el CORE y los conmutadores capa 3 lo que permitió iniciar el plan de direccionamiento identificando los equipos disponibles, los cuales son:

- Conmutador CISCO Catalyst 6509. Núcleo de la red.
- Conmutador CISCO Catalyst 3750. División TIC.
- Conmutador CISCO Catalyst 3750. Edificio de Santo Domingo.
- Conmutador CISCO Catalyst 3750. Edificio de El Carmen.
- Conmutador CISCO Catalyst 3750. Edificio de Ciencias Contables, Económicas y Administrativas.
- Conmutador CISCO Catalyst 3750. Edificio de laboratorios de Física.
- Conmutador CISCO Catalyst 3750. Edificio de Ingenierías.
- Conmutador CISCO Catalyst 3750. Edificio de Ciencias de la Salud
- Conmutador CISCO Catalyst 3750. Edificio de la Facultad de Ciencias Naturales, Exactas de la Educación FACNED.
- Conmutador CISCO Catalyst 3750. Edificio de la Facultad de Artes

En la tabla 2.1.11, se relacionan los equipos capa 3, con los cuales se cuentan para la implementación del protocolo IPv6, dado que cumplen con los requerimientos de software y hardware necesarios.

**Tabla 2.1.11 Componentes capa 3 identificados para la implementación del protocolo IPv6**

| Equipo capa 3 | Versión IOS | Dependencia |
|---|---|---|
| CISCO Catalyst 6509 | 12.2 (53) | Núcleo de la red |
| CISCO Catalyst 3750 | 12.2 (53) | División TIC |
| CISCO Catalyst 3750 | 12.2 (53) | Edificio de Santo Domingo |
| CISCO Catalyst 3750 | 12.2 (53) | Edificio de El Carmen |
| CISCO Catalyst 3750 | 12.2 (53) | Edificio de Ciencias Contables, Económicas y Administrativas |
| CISCO Catalyst 3750 | 12.2 (53) | Edificios de laboratorios de Física |
| CISCO Catalyst 3750 | 12.2 (53) | Edificio de Ingenierías |
| CISCO Catalyst 3750 | 12.2 (53) | Edificio de Ciencias de la Salud |
| CISCO Catalyst 3750 | 12.2 (53) | Edificio de la FACNED |
| CISCO Catalyst 3750 | 12.2 (53) | Edificio de la Facultad de Artes |

- **Mapas lógicos de acceso a los servicios:**

Para tener más claridad sobre el acceso a la red y a los servicios por parte de los usuarios, se plasman los siguientes mapas lógicos de acceso a estos. En la figura 2.1.2 Se muestra como se accede a internet y a los Servicios Internet institucionales desde la LAN. En la figura 2.1.3 se expone como acceden a los mismos servicios, los usuarios que usan NAT y no pasan a través del proxy. El acceso a los servicios de la Universidad desde Internet se expone en la figura 2.1.4.

**Figura 2.1.2 Acceso a servicios mediante PROXY**

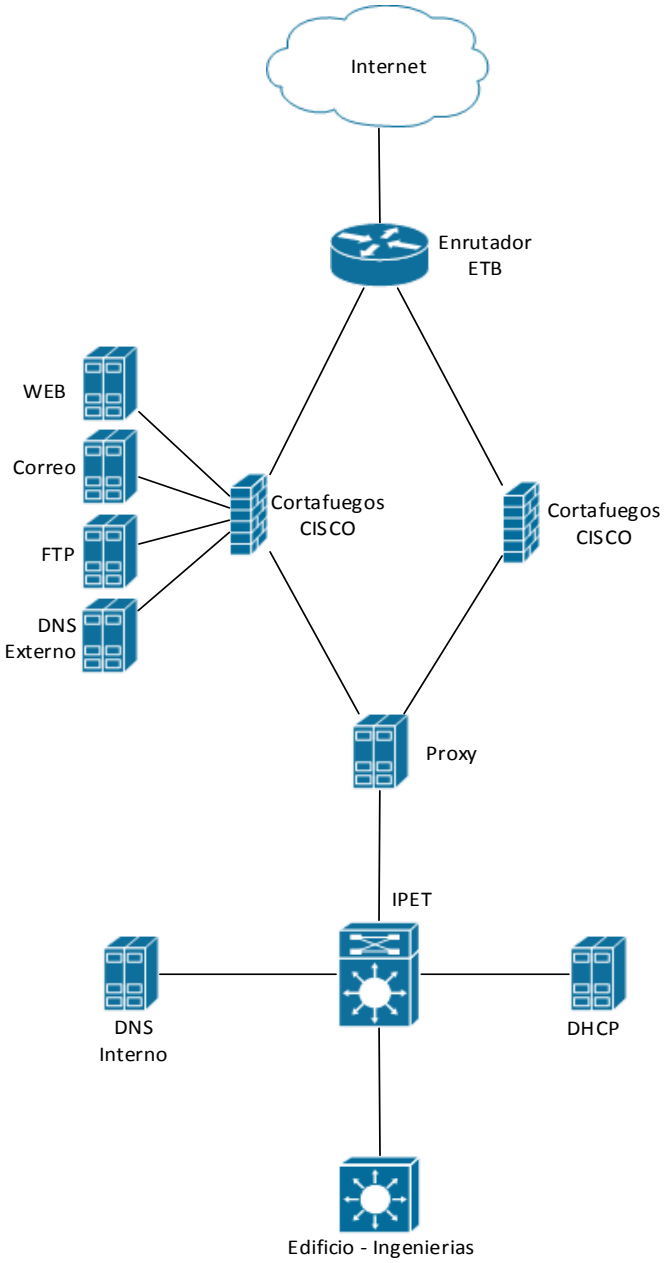


**Figura 2.1.3 Acceso a servicios mediante NAT**

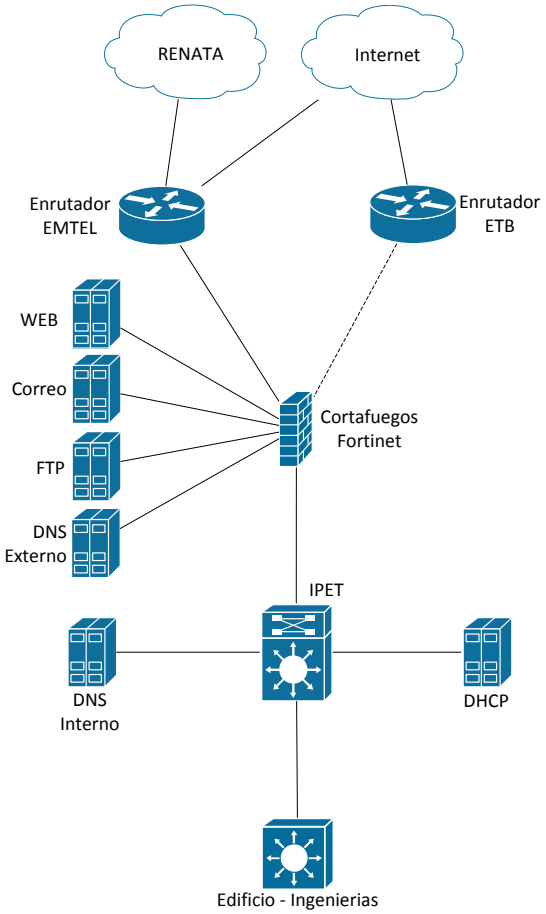


**Figura 2.1.4 Acceso a servicios desde Internet**

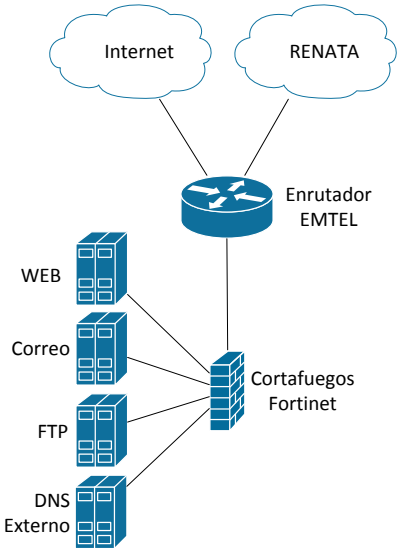



**Tabla 2.1.12 Lista de verificación para la caracterización de la red existente**

| Consideración | Si | No | Observaciones |
|---|---|---|---|
| ¿La topología de red y la infraestructura física, están documentados? | X | | En la figura 2.1.1, se esquematiza la topología de red y estructura física. |
| ¿Las direcciones y nombres de red, se asignan de manera estructurada y están documentadas? | X | | En la tabla 2.1.6, se identifican las dependencias/Nodos de red de información de la Universidad del Cauca.<br><br>En la tabla 2.1.9, se identifican el direccionamiento IPv4 en uso de la Universidad del Cauca. |
| ¿Se han recopilado configuraciones de dispositivos de enrutamiento y conmutación? | X | | En la tabla 2.1.10, se identifican los dispositivos Componentes capa 3 identificados para la implementación del protocolo IPv6.<br><br>En la tabla 2.1.8, se identifican las configuraciones generales sobre equipos CISCO Catalyst 3750. |

### 2.1.4 Caracterización del tráfico existente:

En la tabla 2.1.13, se identifican los usuarios y servicios de la red de información de la Universidad del Cauca, de los cuales se reconocen como fuente, los servicios Institucionales e Internet y se reconocen como destino: la Academia y Administrativos.

En las figuras 2.1.2, 2.1.3 y 2.1.4, se muestra las formas de acceso a internet y a los servicios Institucionales, desde la LAN, identificando los destinos u usuarios que acceden a los servicios o fuentes a través de NAT o Proxy.

Siguiendo con el esquema jerárquico de la red planteado, los usuarios o destinos, se ubican después de los conmutadores de acceso y los servicios Institucionales e Internet o fuetes, están sobre el núcleo, como se indica en la tabla 2.1.13.

**Tabla 2.1.13 Identificación de fuentes y destinos de tráfico**

| **Fuentes** | **Servicios Institucionales e internet** |
|---|---|
| Núcleo | |
| Distribución | |
| Acceso | |
| **Destino** | **Academia y Administrativos** |

En las tablas 2.1.14 y 2.1.15 se identifica las dependencias, que conforman la red de información de la Universidad del Cauca y la zona de aplicaciones y/o servicios Internet, consumidos por los usuarios de la misma.

**Tabla 2.1.14 Identificación de dependencias**

| **Dependencia** | **Aplicaciones Utilizadas** |
|---|---|
| División TIC | Correo Electrónico<br>FTP<br>WEB<br>Video conferencia |
| Edificio de Santo Domingo | |
| Edificio de El Carmen | |
| Edificio de Ciencias Contables, Económicas y Administrativas | |
| Edificios de laboratorios de Física | |
| Edificio de Ingenierías | |
| Edificio de Ciencias de la Salud | |
| Edificio de la Facultad de Ciencias Naturales, Exactas de la Educación | |
| Edificio de la Facultad de Artes | |

**Tabla 2.1.15 Identificación de los servicios**

| **Servidor** | **Localización** | **Usuarios** |
|---|---|---|
| Correo Electrónico | DMZ | Academia y |

| | | |
|---|---|---|
| FTP | DMZ | Administrativos ubicados en las dependencias listadas en la Tabla 2.1.13. |
| WEB | DMZ | |
| Video Conferencia | DMZ | |
| Internet | Exterior a la LAN | |

**Tabla 2.1.16 Lista de verificación para la caracterización del tráfico de la red**

| Consideración | Si | No | Observaciones |
|---|---|---|---|
| ¿Se ha identificado las principales fuentes de tráfico y servidores? | X | | En la tabla 2.1.14 se identifican las principales fuentes de tráfico y servicios |

Toda la información recopilada, en la etapa de **Identificación de las necesidades y objetivos de la Universidad del Cauca**, fue suministrada por el Ingeniero Jaime Martínez, jefe del área de IR de la división TIC de la Universidad del Cauca, mediante la entrevista referenciada en el anexo B.

## 2.2 FASE DE DISEÑO LÓGICO

Para la fase de diseño se debe interactuar con la administración de la red para la validación de este, de acuerdo a lo anterior se sigue:

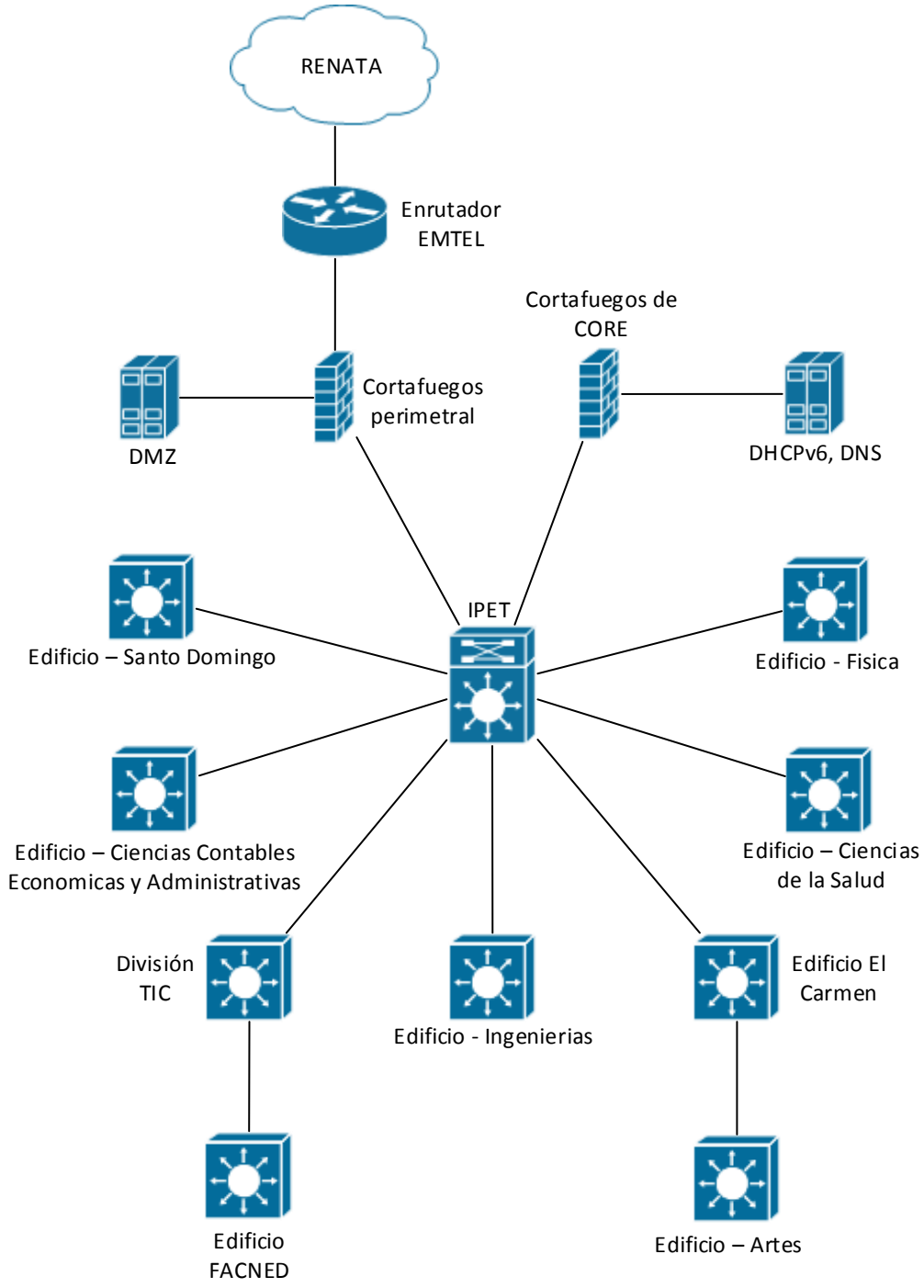
### 2.2.1 Diseño de la topología de red

El diseño de la topología IPv6 se plantea basado en la topología de red IPv4 (ver figura 2.1.1), la caracterización de la red existente y las limitaciones y metas establecidas previamente, sobre esta se verifica que de todos los equipos con IOS actualizado el único equipo de enrutamiento que no soporta la habilitación del nuevo protocolo es el ubicado en el edificio de la *unidad de Salud.* También se debe excluir el equipo de la *División Financiera* debido a políticas comprendidas anteriormente.

En el numeral 2.1.3 se hace referencia dos cortafuegos de la Universidad sin embargo después de entregado el proyecto, la Institución realizo una inversión en este apartado lo cual afecta la topología inicial. En este nuevo esquema de red se tienen dos cortafuegos, uno perimetral que protege la red de servidores y permite administrar la navegación WEB de los usuarios, el segundo es el cortafuegos de CORE que protege servidores de bases de datos y el tráfico del área financiera. En este último también se ubican los servidores DHCP y DNS internos

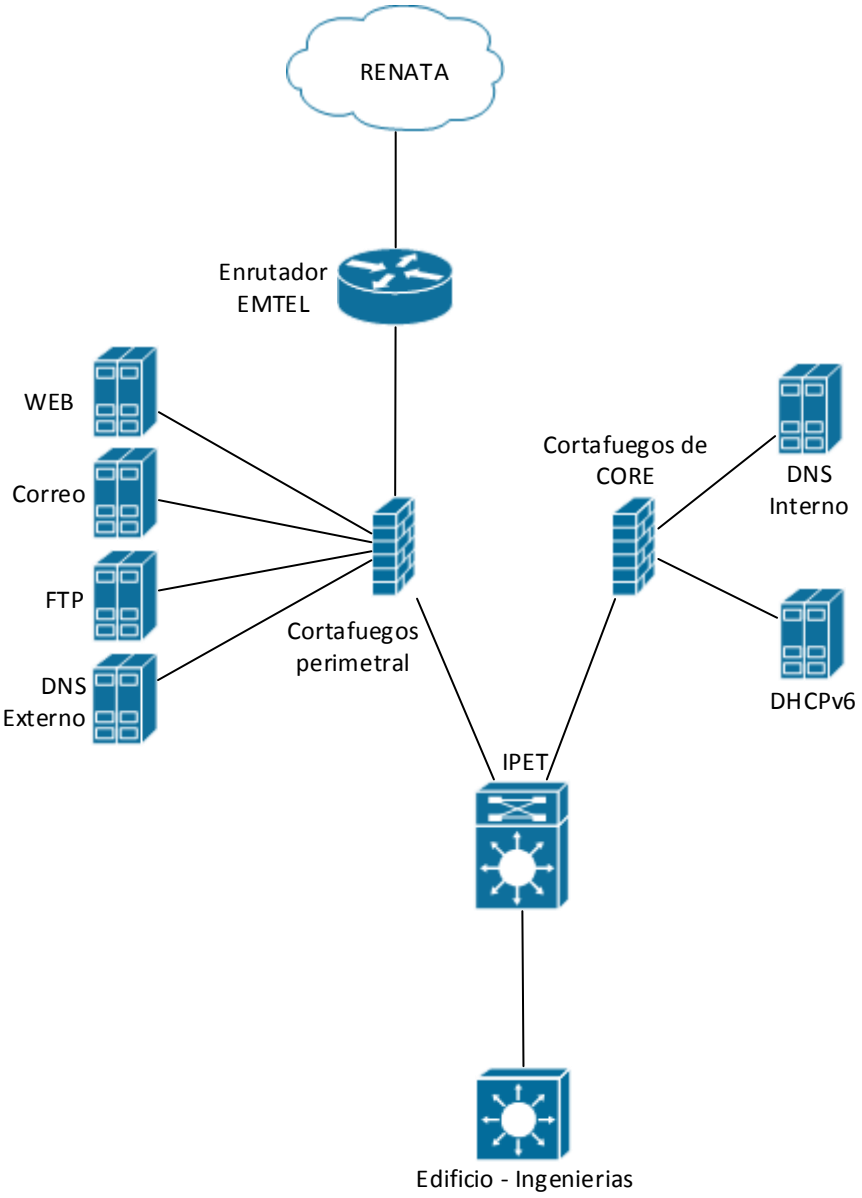
De lo anterior se obtiene la siguiente topología lógica de red IPv6 para la Universidad del Cauca compuesta por el dispositivo de Núcleo, nueve equipos de nivel de distribución, los cortafuegos de referencia Fortigate 800C y 1000C y el enrutador del ISP EMTEL, previamente aprobada por el *Área de Infraestructura*.

**Figura 2.2.1 Topología de red IPv6**




El acceso a los servicios se visualiza mediante el siguiente mapa lógico de acceso a servicios.

**Figura 2.2.2 Mapa lógico IPv6 de acceso a servicios**




### 2.2.2 Diseño de modelos para direccionamiento y denominación

La fase de diseño del direccionamiento se enfocó en las direcciones de tipo unicast globales proveyendo así una solución que permite a los usuarios finales llámense host o servidores poder tener conexión con redes externas, en este caso las académicas. El centrarse en este cometido no quiere decir que internamente no se haga uso de las direcciones de enlace local ya que estas hacen parte de los fundamentos de IPv6 y se usan en el protocolo de Descubrimiento de Vecinos (ND, *Neighbor discovery*) y en DHCPv6.

El tener definido el alcance que tendría el nuevo protocolo sobre la red de la institución precisó el tamaño del prefijo a usar para el plan de direccionamiento. El factor más crítico en la disponibilidad de direcciones en toda la red interna es la LAN para la cual se tiene un estimado de 4000 equipos que hacen uso de las 256 subredes clase C que provee el plan de IPv4. Estas VLANs, sumadas a las de los servicios exponen una red en la que no se ha hecho uso del Enrutamiento entre Dominios Sin Clase (CIDR, *Classless Inter-Domain Routing*) y en la cual algunas de estas ya presentan escases como la subred 192.168.210.0/24 que ya no tiene espacio disponible.

Si bien en un principio se recomendaba la asignación de prefijos de longitud /48 [18], en marzo de 2011 se publica la RFC 6177 que propicia el uso de CIDR y da libertad a los Registros regionales de Internet (RIR, *Regional Internet Registries*) y a los ISPs para que hagan asignación de redes sin importar la longitud, siempre y cuando se respeten los principios de asignación de bloques lo suficientemente grandes para el tráfico actual y planeado a futuro de una institución. De lo anterior hace uso el alma matér al pertenecer a la Red Nacional Académica de Tecnología Avanzada (RENATA), corporación a la cual le fue asignado el bloque 2001:13f8::/32, este bloque se segmento para todas las redes regionales. El sub-bloque 2001:13f8:8050::/40 lo obtuvo la Red Universitaria de Popayán (RUP) del cual la Universidad del Cauca registra el prefijo 2001:13f8:8050::/44. Al tener un bloque de direcciones IPv6 asignado, dado el tiempo limitado del proyecto y costos en los que se incurre al solicitar un bloque propio al registro regional, se opta por continuar el plan de direccionamiento IPv6 haciendo uso de éste.

Partiendo del bloque de direcciones obtenido previamente por la institución, se elige hacer uso solamente del prefijo 2001:13f8:8050::/48 dejando así disponibles para futuros proyectos de investigación y de conexión hacia otras sedes universitarias 15 subredes desde la 2001:13f8:8051::/48 hasta la 2001:13f8:805F::/48.

Como referente para la segmentación del prefijo se usa la RFC 5375 que persuade a no dividirlo más allá del /64 para uso de sub-redes debido a que violaría varias características de IPv6, incluyendo el protocolo de descubrimiento de vecinos (ND, Neighbor Discovery), Mobile IPv6, multihomming para IPv6 entre otras [19]. Esta recomendación también hace énfasis en el uso de redes /64 para cada segmento, en el caso de la Universidad se aplica a cada VLAN. Así mismo aclara que para enlaces punto-punto entre enrutadores donde no se necesitan las características anteriormente mencionadas se puede hacer uso de prefijos /126.

Teniendo en cuenta lo anterior se establece un esquema que usa los bits del 49 al 64 (cuarto cuarteto de izquierda a derecha) de la dirección para la creación de cuatro niveles de red (un nivel por cada digito hexadecimal del cuarteto), que incrementa gradualmente de a cuatro bits (un digito) como se muestra a continuación con ejemplos, los números del uno al nueve indican un grupo de bits y su asignación.

**Tabla 2.2.1 Esquema de dirección para la LAN**

| 2 | 0 | 0 | 1 | : | 1 | 3 | f | 8 | : | 8 | 0 | 5 | 0 | : | 6 | 1 | 0 | 1 | : | : | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | 2 | | | | | 3 | | | 4 | | 5 | 6 | 7 | 8 | | | 9 |

- 5, 6, 7 y 8 conforman el cuarto cuarteto mencionado

1. Red /16 de uso comercial
2. Red /32 asignada a RENATA
3. Red /44 asignada a la Universidad del Cauca por RENATA
4. Red /48 Para despliegue del actual proyecto
5. Sub-red /52 asignada como segmento a un edificio
6. Sub-red /56 asignada como segmento a dependencias dentro de un mismo edificio
7. Sub-red / 60 asignada como segmento a Diferentes laboratorios dentro de una dependencia
8. Sub-red asignada como segmento a cada una de las VLANs
9. Dirección IPv6 asignada a un equipo dentro de una VLAN

Para la asignación de la sub-redes ::/52 a edificios, estos se enumeran así:

0. Enlaces punto-punto
1. Ciencias de la Salud
2. VRI
3. Santo Domingo
4. Viejo Liceo
5. Contaduría
6. Ingenierías
7. El Carmen
8. IPET

La asignación de los dígitos de dependencias y laboratorios es ambigua debido a la estructura de cada uno. La concesión para cada VLAN (::/64) se sigue de acuerdo a la siguiente numeración brindada por el área de infraestructura, de esta se excluye el rango de edificio número cero ya que es asignado a enlaces punto-punto y estos se tratan aparte:

1. VLAN Estudiantes
2. VLAN docentes
3. VLAN Administrativos
4. VLAN Inalámbrica

5. VLAN Videoconferencia
6. VLAN Servidores
7. VLAN Sistemas de Información
8. VLAN Cámaras
9. VLAN VoIP
1. VLAN Biométrica

A cada una de estas VLANs se le asigna la primera dirección de su rango.

Para los servicios se desarrolló otro esquema:

**Tabla 2.2.2 Esquema de direcciones para servidores**

| 2 | 0 | 0 | 1 | : | 1 | 3 | f | 8 | : | 8 | 0 | 5 | 0 | : | f | 6 | 0 | 1 | : | : | 1 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | | | | | 2 | | | | | 3 | | | 4 | | 5 | 6 | 7 | 8 | | | 9 |

1. Red /16 de uso comercial
2. Red /32 asignada a RENATA
3. Red /44 asignada a la Universidad del Cauca por RENATA
4. Red /48 Para despliegue del actual proyecto
5. Sub-red /52 asignada a servidores
6. Sub-red /56 asignada por tipo de cortafuegos
7. Sub-red /60 asignada por tipo de servicios
8. Sub-red /64 asignada a cada VLAN de servicios
9. Dirección IPv6 asignada a un servidor

La asignación de los dígitos por tipo de cortafuegos (::/56) se divide en dos:

1. Cortafuegos perimetral
2. Cortafuegos de CORE

Los dígitos para los tipos de servidores se conceden de la siguiente manera:

1. Servicios WEB
2. FTP
3. DNS
4. DHCP
5. Correo

Para ver con mayor detalle el direccionamiento IPv6 a aplicar en la red de la Universidad del Cauca y las direcciones asignadas a cada VLAN en la LAN y a cada VLAN de servicios revisar el anexo A.

### 2.2.3 Selección de protocolos de conmutación y enrutamiento

Como se plantea en el numeral 2.1.3, el área de infraestructura determinó que del mismo modo en que se administra la red IPv4, en IPv6 se debe manejar enrutamiento estático en cada equipo de red de capa tres. En consecuencia el trabajo en este apartado se concentra en determinar las rutas en cada equipo. El nuevo protocolo también soporta sumarizacion de rutas por lo tanto se debe prever la utilización de la menor cantidad de rutas posibles.

Para los equipos de nivel de distribución se tienen rutas apuntando siempre hacia el Núcleo de la red, estas se muestran en la tabla 2.2.3 a continuación,

**Tabla 2.2.3 Rutas estáticas en cada equipo de distribución**

| Red | | Puerta de enlace |
|---|---|---|
| • Ciencias de la Salud:<br>Ruta por defecto | | 2001:13f8:8050:201::1 |
| • Santo Domingo<br>Ruta por defecto | | 2001:13f8:8050:203::1 |
| • División TIC | • Ruta por defecto | 2001:13f8:8050:204::1 |
| | • 2001:13f8:8050:4200::/56 | 2001:13f8:8050:204::6 |
| | • 2001:13f8:8050:542::/64 | 2001:13f8:8050:204::6 |
| | • FACNED<br>Ruta por defecto | 2001:13f8:8050:204:5 |
| • Contaduría<br>Ruta por defecto | | 2001:13f8:8050:205::1 |
| • Ingenierías<br>Ruta por defecto | | 2001:13f8:8050:206::1 |
| • El Carmen | • Ruta por defecto | 2001:13f8:8050:207::1 |
| | • 2001:13f8:8050:7300::/56 | 2001:13f8:8050:207::12 |
| | • 2001:13f8:8050:573::/64 | 2001:13f8:8050:204::12 |
| | • Artes<br>Ruta por defecto | 2001:13f8:8050:207::11 |
| • Física<br>Ruta por defecto | | 2001:13f8:8050:208::1 |

El equipo de Núcleo debe tener una ruta hacia los cortafuegos y las distintas rutas de la VLANs de cada equipo de distribución:

**Tabla 2.2.4 Rutas estáticas a configurar en el CORE**

| Red | Puerta de enlace |
|---|---|
| Ruta por defecto hacia | 2001:13f8:8050:200::1 |
| Red 2001:13f8:8050:1000::/52 | 2001:13f8:8050:201::2 |
| Red 2001:13f8:8050:3000::/52 | 2001:13f8:8050:203::2 |
| Red 2001:13f8:8050:4000::/52 | 2001:13f8:8050:204::2 |
| Red 2001:13f8:8050:5000::/52 | 2001:13f8:8050:205::2 |
| Red 2001:13f8:8050:6000::/52 | 2001:13f8:8050:206::2 |
| Red 2001:13f8:8050:7000::/52 | 2001:13f8:8050:207::2 |
| Red 2001:13f8:8050:8000::/52 | 2001:13f8:8050:208::2 |
| Red 2001:13f8:8050:f200::/56 | 2001:13f8:8050:200::10 |
| Red 2001:13f8:8050:510::/60 | 2001:13f8:8050:201::2 |
| Red 2001:13f8:8050:530::/60 | 2001:13f8:8050:203::2 |
| Red 2001:13f8:8050:540::/60 | 2001:13f8:8050:204::2 |
| Red 2001:13f8:8050:550::/60 | 2001:13f8:8050:205::2 |
| Red 2001:13f8:8050:560::/60 | 2001:13f8:8050:206::2 |
| Red 2001:13f8:8050:570::/60 | 2001:13f8:8050:207::2 |
| Red 2001:13f8:8050:580::/60 | 2001:13f8:8050:208::2 |
| Red 2001:13f8:8050:204::4/126 | 2001:13f8:8050:207::2 |
| Red 2001:13f8:8050:207::10/126 | 2001:13f8:8050:208::2 |

Finalmente se tiene el enrutamiento en los cortafuegos, el perimetral debe tener una ruta hacia el enrutador de frontera de EMTEL y rutas hacia la red interna excluyendo los enlaces punto-punto:

**Tabla 2.2.5 Rutas estáticas en el cortafuegos perimetral**

| Red | Puerta de enlace |
|---|---|
| Ruta por defecto | 2001:13f8:8050:101::1 |
| Red 2001:13f8:8050:1000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:3000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:4000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:5000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:6000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:7000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:8000::/52 apuntando hacia | 2001:13f8:8050:200::2 |

El cortafuegos de CORE debe tener una ruta por defecto hacia el perimetral y si debe tener las rutas de los enlaces putno-punto ya que desde estas redes llegan los mensajes “DHCPv6-relay”.

**Tabla 2.2.6 Rutas en el cortafuegos de CORE**

| Red | Puerta de enlace |
|---|---|
| Ruta por defecto hacia | 2001:13f8:8050:200::1 |
| Red 2001:13f8:8050:1000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:3000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:4000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:5000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:6000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:7000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050:8000::/52 apuntando hacia | 2001:13f8:8050:200::2 |
| Red 2001:13f8:8050::/52 apuntando hacia | 2001:13f8:8050:200::2 |

Finalmente se determina que la dirección de *link-local*[4] de cada interfaz o VLAN de los equipos de red se configura como fe80::1, dado que esta no se enruta no se presentan inconvenientes de traslape. Esto ayuda a que usuarios con direcciones configuradas dinámicamente siempre encuentren la misma puerta de enlace predeterminada, facilitando el uso por parte de personal sin experiencia.

### 2.2.4 Desarrollo de estrategias de seguridad

Las estrategias de seguridad para la red IPv6 de la Universidad del Cauca se centran en configuración de rutas y políticas en el cortafuegos. Dado que el nuevo protocolo no hace uso de direcciones privadas no se tiene un método de protección de los equipos de red basado en estas, más que la no publicación de rutas hacia las sub-redes 2001:13f8:8050:200::/56 y 2001:13f8:8050:500::/56.

Un método de seguridad preciso y orientado a los servicios es la configuración de políticas que bloqueen el trafico basado en puertos TCP/UDP. El proyecto contempla la implementación de estas para brindar acceso a los servicios HTTP, SMTP, POP3, IMAP, FTP y DNS externo en la DMZ. A continuación se desglosan permisos de acceso por servicio para los dos cortafuegos.

[4] Link-local. Direcciones Ipv6 de ámbito local que no se pueden enrutar y sirven para las primeras etapas de configuración

**Tabla 2.2.7 Políticas en cortafuegos perimetral**

| Servicio | Política |
|---|---|
| HTTP | • Cualquier red a la IPv6 2001:13f8:8050:f110::/64<br>• Cualquier sub-red de la Universidad hacia la WAN |
| SMTP, POP3 e IMAP | • Cualquier red a la IPv6 2001:13f8:8050:f100::f1e7:5/64<br>• Cualquier red a la IPv6 2001:13f8:8050:f100::5/64<br>• Cualquier sub-red de la Universidad hacia la WAN |
| FTP | • Cualquier red a la IPv6 2001:13f8:8050:f100::2:1/64<br>• Cualquier red a la IPv6 2001:13f8:8050:f100::f1e7:2/64<br>• Cualquier sub-red de la Universidad hacia la WAN |
| DNS externo | • Cualquier red a la IPv6 2001:13f8:8050:f100::3:1/64<br>• Cualquier red a la IPv6 2001:13f8:8050:f100::3:2/64 |

**Tabla 2.2.8 Políticas en cortafuegos de CORE**

| Servicio | Política |
|---|---|
| DHCPv6 | • Cualquier sub-red de la Universidad hacia la IPv6 2001:13f8:8050:f230::4:1/64 |
| DNS interno | • Cualquier sub-red de la Universidad hacia la IPv6 2001:13f8:8050:f230::1:1/64<br>• Cualquier sub-red de la Universidad hacia la IPv6 2001:13f8:8050:f230::1:2/64 |

## 2.3 PRUEBAS Y OPTIMIZACIÓN

### 2.3.1 Pruebas del diseño de red

El aspecto de las pruebas para este proyecto se enfoca en verificar el funcionamiento en un ambiente real de poca carga de tráfico y en momentos que no cause mayor coyuntura con los usuarios sin alguna falla en la red IPv4 se presenta. El plan de pruebas y despliegue programado con los ingenieros Jaime Martínez y Andrés Zúñiga, administradores de la red, contempla que si ningún inconveniente se presenta a medida que se vaya implementando se sigue adelante con el procedimiento, sin embargo si un problema se presenta se detienen las pruebas y despliegue para verificar la causa. El orden a seguir para la configuración es el siguiente:

1. Artes
2. El Carmen
3. Núcleo (IPET)
4. Ciencias de la Salud
5. Contaduría
6. Santo Domingo
7. División TIC
8. FACNED
9. Ingenierías

Para el procedimiento en cada equipo se usan una serie de comandos del sistema operativo de CISCO como lo son:

- Configuración global

    - sdm prefer dual-ipv4-and-ipv6 routing

      Aun cuando el sistema Operativo de los equipos soporta el protocolo, por defecto se encuentra desactivado. Este comando lo activa pero se debe tener cuidado ya que es necesario reiniciar el equipo para terminar el proceso.

    - ipv6 unicast-routing

      En la configuración del terminal se debe introducir este comando para habilitar el enrutamiento de paquetes IPv6.

    - ipv6 general-prefix WORD 2001:13f8:8050:6100::/56

      Este comando fue desarrollado por CISCO y no es un estándar de IPv6 pero si es muy conveniente para la configuración ya que permite definir una serie de prefijos globales dentro del equipo lo cual facilita asignar la dirección a una interfaz o VLAN concatenándola con los primeros. Hacer cambios masivos de direcciones en las interfaces que usen uno de estos es mucho más ágil debido a que solo se debe cambiar el prefijo y automáticamente todas las direcciones se actualizan. La palabra WORD debe ser reemplazada por el nombre con el cual se desee identificar.

    - ipv6 cef

      Como complemento del anterior comando.

    - ipv6 route 2001:13f8:8050::x/xx 2001:13f8:8050:x::x

      Comando para asignar rutas estáticas, similar a IPv4, se debe poner primero la red seguida de la dirección por la cual se conecta. Las X deben ser

reemplazadas por dígitos correspondientes a direcciones y redes de la Universidad.

- ipv6 ::/0 2001:13f8:8050:x::x

Comando para asignar rutas por defecto, como se hace en IPv4 se completa con la dirección del próximo salto. Las X deben ser actualizadas a la dirección correcta del enlace punto-punto.

- Interfaz

  - ipv6 address WORD ::1:0:0:0:1/64

  Este comando es el que concatena un prefijo global del equipo con una parte de red de la interfaz, la palabra WORD debe ser reemplazada por la misma con la cual se identificó el prefijo, los cuatro puntos sirven como unión y no como resumen de ceros. Cabe aclarar que esta no es la manera por defecto de agregar direcciones, sin embargo si es la que se sigue en el proyecto.

  - ipv cef

  Permite la concatenación de los prefijos y los segmentos de red.

  - ipv6 nd router-preference high

  Asigna la prioridad más alta al anuncio de *router advertisement*[5].

  - ipv6 add fe80::1 link-local

  Cambia la dirección de *link-local* de la interfaz. Esta dirección es la anunciada por *router advertisement* como puerta de enlace predeterminada para los equipos con configuraion dinámica. Cada VLAN de la Universidad debe tener esta dirección.

Debido a la confidencialidad con que se tratan las configuraciones de los equipos de red no se muestra la configuración de los diez dispositivos involucrados.

En lo referente a las configuraciones del cortafuegos, el ingeniero Fabián Mera está al frente de la configuración definida en el numeral 2.2.3 y 2.2.4 en lo correspondiente a este equipo. Debido a la delicadeza del acceso, la información y la configuración de este, el ingeniero adapta las configuraciones del plan de seguridad a la interfaz de configuración del Fortinet 310B.

[5] Router advertisement. Mensajes de anuncio de ruta. Hace parte del protocolo Neighbor Discovery

Como verificación de que se tiene una red IPv6 institucional con acceso a la WAN dispuesta para la implementación de los servicios Internet IPv6, se despliega una serie de ilustraciones que muestran el comando *tracert*[6] desde un equipo terminal con sistema operativo Windows. Este comando muestra la ruta realizada por un paquete ICMPv6.

**Figura 2.3.1 Traza de ruta entre VLAN administrativa en División TIC y VLAN docentes en Salud**

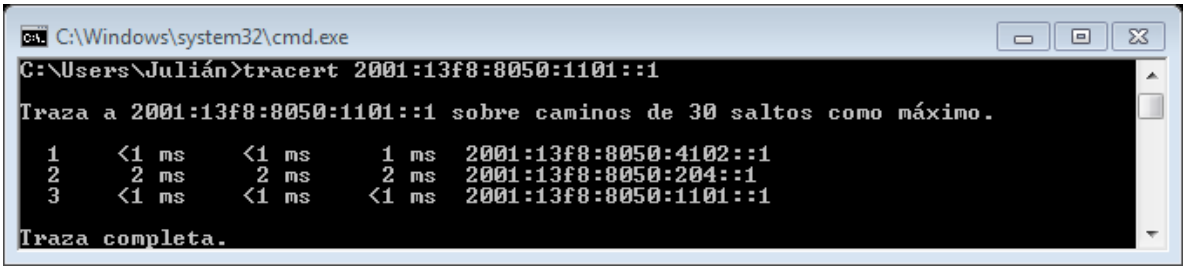



**Figura 2.3.2 Traza de ruta entre VLAN administrativa en División TIC y VLAN docentes en Santo Domingo**

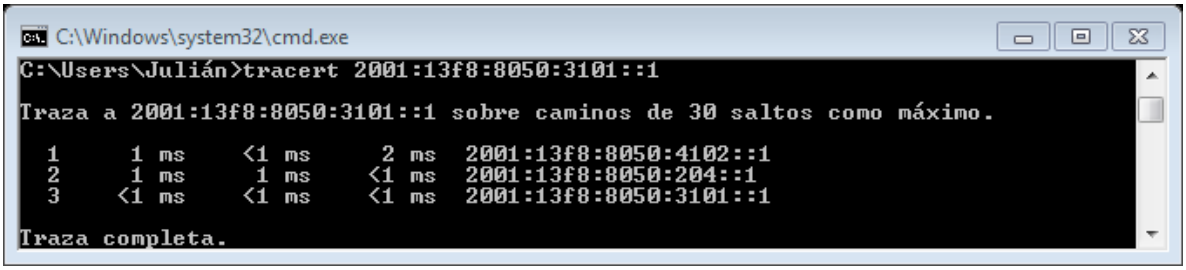
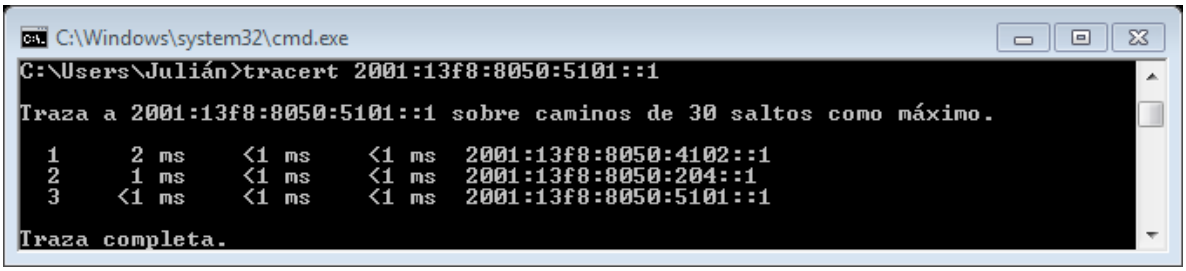



**Figura 2.3.3 Traza de ruta entre VLAN administrativa en División TIC y VLAN docentes en Ciencias Contables**




[6] Tracert. Funcionalidad de la ventana de comandos de Windows para rastrear paquetes ICMP.

**Figura 2.3.4 Traza de ruta entre VLAN administrativa en División TIC y VLAN docentes en Ingenierías**

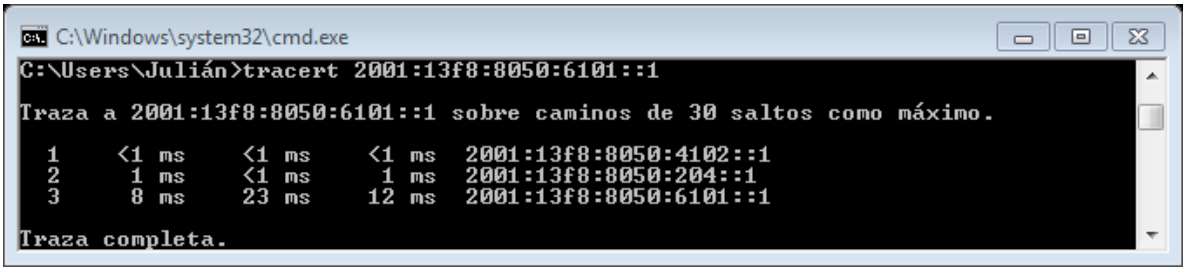



**Figura 2.3.5 Traza de ruta entre VLAN administrativa en División TIC y VLAN docentes en El Carmen**


**Figura 2.3.6 Traza de ruta entre VLAN administrativa en División TIC y VLAN docentes en Artes**


**Figura 2.3.7 Traza de ruta entre VLAN administrativa en División TIC y VLAN docentes en Física**

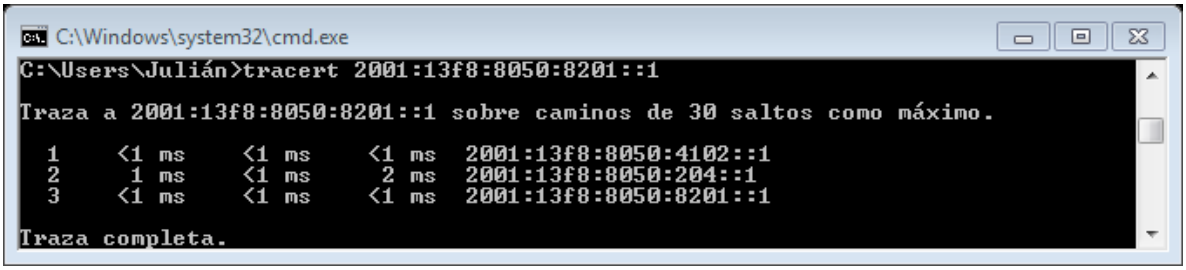
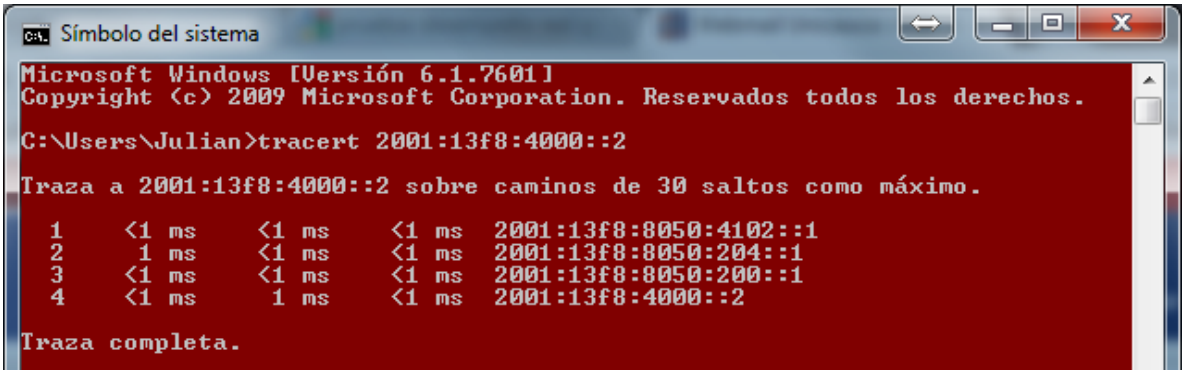


**Figura 2.3.8 Traza de ruta entre VLAN administrativa en División TIC y enrutador de frontera de EMTEL**



# 3 IMPLEMENTACIÓN DE LOS SERVICIOS INTERNET IPv6

Los Servicios Internet de la Universidad del Cauca, administrados por el área SSI (Servidores y Servicios Internet), perteneciente a la división TIC, son de vital importancia para la Institución, siendo el soporte de muchos otros procesos en facultades y dependencias, por lo cual, se manejan unas políticas internas, que restringen la mención detallada del estado de algunos servidores. Esto debido, a la criticidad de algunas áreas. Para representar mejor lo anterior, el área SSI concibe la distribución de los servicios en cinco zonas plenamente establecidas como se indica en la tabla 3.0.1.

**Tabla 3.0.1 Identificación de Zonas de Servidores de la Universidad del Cauca**

| **Zonas de Servidores de la red de Información de la Universidad del Cauca** | |
|---|---|
| 1 | Zona desmilitarizada (DMZ*, Demilitarized Zone*) |
| 2 | Zona de Bases de datos |
| 3 | Zona de Aplicaciones |
| 4 | Zona Externa |
| 5 | Zona de Proxy |

Debido a las restricciones mencionadas y a los objetivos del proyecto, solo se tuvo acceso a las zonas: DMZ, que contiene los servicios que serán alcanzados desde la LAN y desde la WAN, estos son el DNS externo, portal WEB de la Universidad y la página del correo Institucional, también está el servidor de Transferencia de Archivos (FTP, File Transfer Protocol) y el correo electrónico. Adicional a estas, hay una zona interna, en la cual se controlan el DHCP y el DNS interno. Se define como servicios Institucionales el DNS, Web, FTP, Correo, DHCPv6 y como servicios de alcance global el Web, FTP y Correo. Esta información se resume en la tabla 3.0.2.

.

**Tabla 3.0.2 Identificación de servicios por zona**

| **Zona** | **Servicios** | **Alcance** |
|---|---|---|
| DMZ<br><br>(Servicios Accesados desde la LAN/WAN). | DNS Externo | Institucional |
| | Portal WEB de la Universidad del Cauca | Institucional – Global |
| | FTP | Institucional – Global |
| | Correo Electrónico | Institucional – Global |
| Proxy | Servidores Proxy | Institucional |
| Interna | DHCP | Institucional |
| | DNS Interno | Institucional |

El estado de cada uno de los servicios IPv4 de la Universidad, se debe analizar por separado, ya que estos, no se encuentran en una plataforma unificada, ante esto, se encuentran diferentes versiones del kernel de Linux, del *Service Pack* de *Windows Server* y diferentes configuraciones para cada servicio.

De acuerdo a lo establecido en el Capítulo I, para la implementación del protocolo IPv6, sobre los servicios Internet de la Universidad del Cauca, se utiliza el Ciclo de Deming o *PDCA,* el cual, describe a continuación cada una de sus fases aplicadas, tanto para servidores con sistema operativo Linux o Windows Server 2008:

La implementación de los servicios anexada a este documento, se considera, tanto para ambientes Linux como Windows, con la intención que sea utilizada y aplicada de acuerdo a las necesidades de la División de TIC de la Universidad del Cauca y todo aquel que utilice este documento como guía para la implementación de los servicios Internet con soporte IPv6.

Posterior al diseño de red e implementación de los Servicios Internet IPv6, la Universidad del Cauca hizo realizo cambios sobre la infraestructura de red como se menciona en el numeral 2.2.1. Estas modificaciones afectaron directamente el plan de direccionamiento inicial planteado en el anexo A, a continuación se presenta la asignación real de direcciones a los servidores, es de resaltar que esto se debe a que algunos servicios comparten la VLAN en la que se alojan.

**Tabla 3.0.3 Asignación de direcciones a servidores**

| Servidor | Dirección IPv6 |
|---|---|
| Portal de la Universidad | 2001:13f8:8050:f110::2 |
| FTP (Odin) | 2001:13f8:8050:f100::2:1 |
| Correo (Afrodita) | 2001:13f8:8050:f100::5:1 |
| DHCP (Orestes) | 2001:13f8:8050:f230::4:1 |
| DNS (Cronos) | 2001:13f8:8050:f230::1:1 |
| DNS (Hades) | 2001:13f8:8050:f230::1:2 |
| DNS1 | 2001:13f8:8050:f100::3:1 |
| DNS 2 | 2001:13f8:8050:f100::3:2 |
| Server (Windows Server) | 2001:13f8:8050:f100::f1e7:1 |
| FTP (Windows Server) | 2001:13f8:8050:f100::f1e7:2 |
| OWA (Correo Windows Server) | 2001:13f8:8050:f100::f1e7:5 |
| DHCP (Linux) | 2001:13f8:8050:f230::4:10 |

## 3.1 Servicio DHCP

El servicio DHCPv6 en la universidad no tiene ningún avance por lo tanto se debe hacer una instalación de un servidor Linux para este propósito y verificar el estado del servidor DHCP sobre Windows Server que se tiene inicialmente para IPv4.

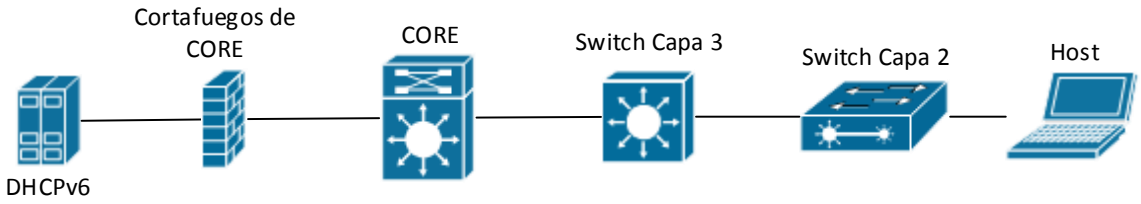
El objetivo es que el servidor con Windows siga operando como principal y el de Linux solo tenga la capacidad de asignar direcciones en su subred. Lo anterior debido a la configuración sobre los equipos de red de nivel de distribución en la cual se debe especificar un "DHCPv6-relay" el cual enruta las solicitudes de DHCP hacia el servidor. Al tener claro el esquema de este servicio se configura previo a la implementación cada VLAN en cada uno de los conmutadores capa 3 mediante la sentencia:

***# ipv6 dhcp relay destination 2001:13f8:8050:f230::4:1 giga 1/0/48***

Esta línea asegura que todas las solicitudes de DHCPv6 que se reciban por la interfaz de una VLAN van a ser enrutadas hacia el servidor Windows por la interfaz que conecta el respectivo conmutador con el CORE.

De acuerdo a la fase de diseño de la topología de red se tiene puntualmente el siguiente esquema para el acceso al servicio.

**Figura 3.1.1 Acceso a servicio DHCPv6**




**Sobre Linux:**

- **Planear:** El objetivo es implementar el servicio DHCPv6 sobre Linux quedando este en producción con un perfil de investigación y desarrollo por lo tanto se configuran unos ámbitos específicos.
  Debido a que este servicio sobre esta plataforma es nuevo se inicia con la instalación del servidor y en concordancia con el plan de direccionamiento planteado, en la sección 2.2.2, se define que la dirección IPv6 a configurar sobre la interfaz del servidor será 2001:13f8:8050:f230::4:10. Esta información se resume en la tabla 3.1.2.

**Tabla 3.1.1 Configuraciones IPv6, previas, para el servidor DHCPv6, bajo Linux**

| Servicio | Sistema Operativo | IPv6 |
|---|---|---|
| DHCPv6 ISC-DHCP 4.1.0 | Debian 6.1.2 – Linux 2.6.26 | 2001:13f8:8050:f230::4:10 |

Teniendo esta información se planea que ámbitos se van a publicar y la información que delega el servidor como los rangos de direcciones, los servidores de nombres de dominio, los servidores de tiempo, intervalos de actualización, etc Esta información se muestra en las tablas 3.1.3 y 3.1.4, la primera muestra los ámbitos que se publicaran asignados a una VLAN y la segunda especifica la información de DNS que se publicara.

**Tabla 3.1.2 Ámbitos a configurar en DHCPv6 sobre Linux**

| Ambito | VLAN | Direcciones disponibles | Direcciones a asignar |
|---|---|---|---|
| 2001:13f8:8050:4102::/64 | Admin – División TIC | 18,45 trillones | 5 |
| 2001:13f8:8050:4802::/64 | Admin – DARCA (temporal) | 18,45 trillones | 10 |
| 2001:13f8:8050:f230::/64 | Servidores DHCP | 18,45 trillones | 1 |

.

**Tabla 3.1.3 Información anexa a DHCPv6 sobre Linux**

| | |
|---|---|
| Servidor DNS | 2001:13f8:8050:f230::1:1 |
| | 2001:13f8:8050:f230::1:2 |
| Tiempo de concesión | 1 día |
| Dominio de búsqueda | Unicauca.edu.co |

- **Hacer:** Se configura la interfaz de red con la dirección IPv6 planeada, esta configuración se explica de manera genérica en el anexo XXXX.

Posteriormente se procede a instalar y configurar el servicio ISC-DHCP como se muestra en el anexo C.1, de acuerdo a los ámbitos y datos planeados en la fase anterior, esta configuración se muestra en la figura 3.1.2. Adicionalmente se configura el cortafuegos para que permita el tráfico de este protocolo desde la Intranet hacia la sub-red del servidor.

**Figura 3.1.2 Configuración dhcpd6.conf**

```
authoritative;
default-lease-time      86400;
max-lease-time  86400;
log-facility local7;
option dhcp6.name-servers 2001:13f8:8050:f230::1:1, 2001:13f8:8050:f230::1:2;
option dhcp6.domain-search "unicauca.edu.co";
option dhcp6.info-refresh-time 300;
option dhcp6.preference 255;


subnet6 2001:13F8:8050:4802::/64 {
        # Range para los clientes 1024 estaciones
            range6 2001:13F8:8050:4802::10 2001:13F8:8050:4802::19;
}

subnet6 2001:13F8:8050:4102::/64 {
        # Range para los clientes 1024 estaciones
            range6 2001:13F8:8050:4102::10 2001:13F8:8050:4102::19;
}

subnet6 2001:13F8:8050:f230::/64 {
        # Range para los clientes 1 estaciones
            range6 2001:13F8:8050:f230::4:10 2001:13F8:8050:f230::4:10;
}
```

- **Verificar:** Debido a que este servidor no responde a la Intranet se debe hacer una prueba limitada y específica sobre la VLAN de administrativos en la división TIC. Esta prueba consiste en configurar el DHCP-relay en el conmutador de esta división enrutando el tráfico de este protocolo hacia la dirección IPv6 “2001:13f8:8050:f230::4:10”. Lo anterior confirma la asignación de direcciones para este ámbito.
- **Actuar:** Se deshabilita el esquema de prueba de la fase anterior y se deja el servidor encendido y operando con disponibilidad de ser puesto en producción sujeto a necesidades del área SSI.

**Sobre Windows Server:**

- **Planear:** el objetivo es implementar el servicio sobre el mismo servidor que soporta IPv4, por lo tanto se debe analizar el estado del equipo inicial, esto se muestra en la tabla 3.1.5.

**Tabla 3.1.4 Información técnica del servidor DHCP, bajo Windows Server**

| | |
|---|---|
| **Nombre** | orestes |
| **Sistema Operativo** | Windows Server 2003 SP2 |
| **Software** | Aplicación nativa para servicio DHCP |
| **IPv4** | 172.16.255.185 |

De esta tabla se infiere que se debe empezar por la actualización del sistema operativo debido a la no compatibilidad de este con el nuevo protocolo de red. En la tabla 3.1.6 se resumen los requerimientos mínimos y plataforma utilizada por el servidor inicial.

**Tabla 3.1.5 Validación del soporte IPv6 sobre el servidor DHCPv6, bajo Windows Server**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Windows Server 2008 o superior | Windows Server 2003 SP2 | No Cumple |
| **DHCP** | Aplicación nativa | ---------- | ---------- |

Teniendo clara esta tabla el área SSI decidió actualizar todo el servidor sobre el cual estaba. En la tabla 3.1.7 se presenta la información básica del nuevo equipo adicional al direccionamiento asignado previamente.

**Tabla 3.1.6 Configuraciones IPv6, previas, para el servidor DHCPv6, bajo Windows Server**

| Servicio | Sistema Operativo | IPv6 |
|---|---|---|
| DHCPv6 Nativo | Windows Server 2008 SP2 | 2001:13f8:8050:f230::4:1 |

- **Hacer:** Como primera actividad de esta fase se lleva a cabo la actualización del sistema operativo y migración de los ámbitos IPv4, estos pasos no se especifican debido a que están fuera de los objetivos del proyecto y se realizan como acciones complementarias.

  Una vez se tiene un servidor con los requerimientos cumplidos se lleva a cabo la configuración de la interfaz de red con la dirección definida en la fase anterior. Este proceso se explica en general para servidores Windows server en el anexo C.2.
  Esta fase se completa con el despliegue sobre el servidor de cada uno de los ámbitos planeados en la fase anterior.

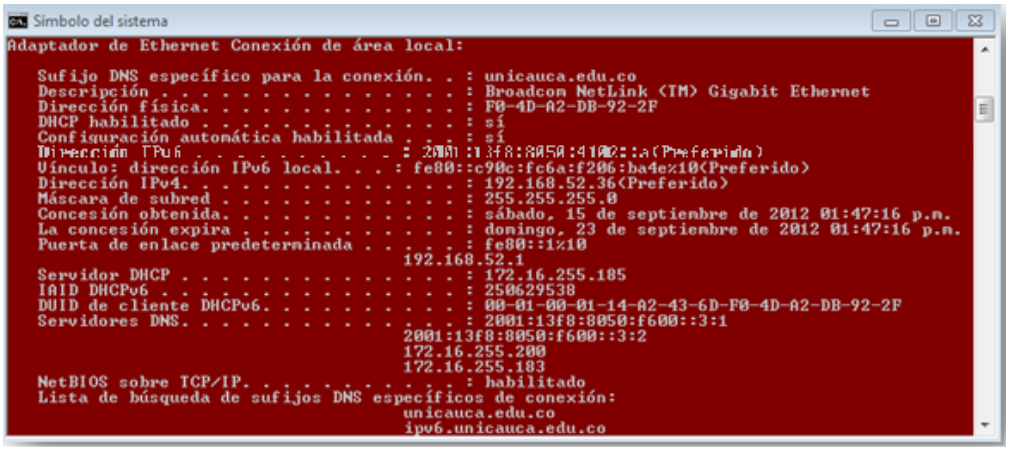
- **Verificar:** Esta fase se lleva a cabo tres ciclos de manera secuencial con la fase de “Actuar”. A continuación se describen las tres instancias.

  1. Se verifica que desde cualquier punto de la red cableada de la Institución se pueda recibir la configuración de una dirección del nuevo protocolo. Sin embargo esta prueba no es exitosa, llevando esto a encontrar que el

sistema operativo Windows Server 2008 tiene un mal funcionamiento en el proceso de respuesta a los mensajes “relay” provenientes de cada uno de los equipos de distribución. Este inconveniente no permite que ningún usuario pueda configurarse una dirección por DHCPv6.

2. Se verifica que una vez aplicado el parche al servidor se asignan correctamente direcciones a usuarios a través de toda la red cableada.

**Figura 3.1.3 Dirección IPv6 asignada por DHCPv6**



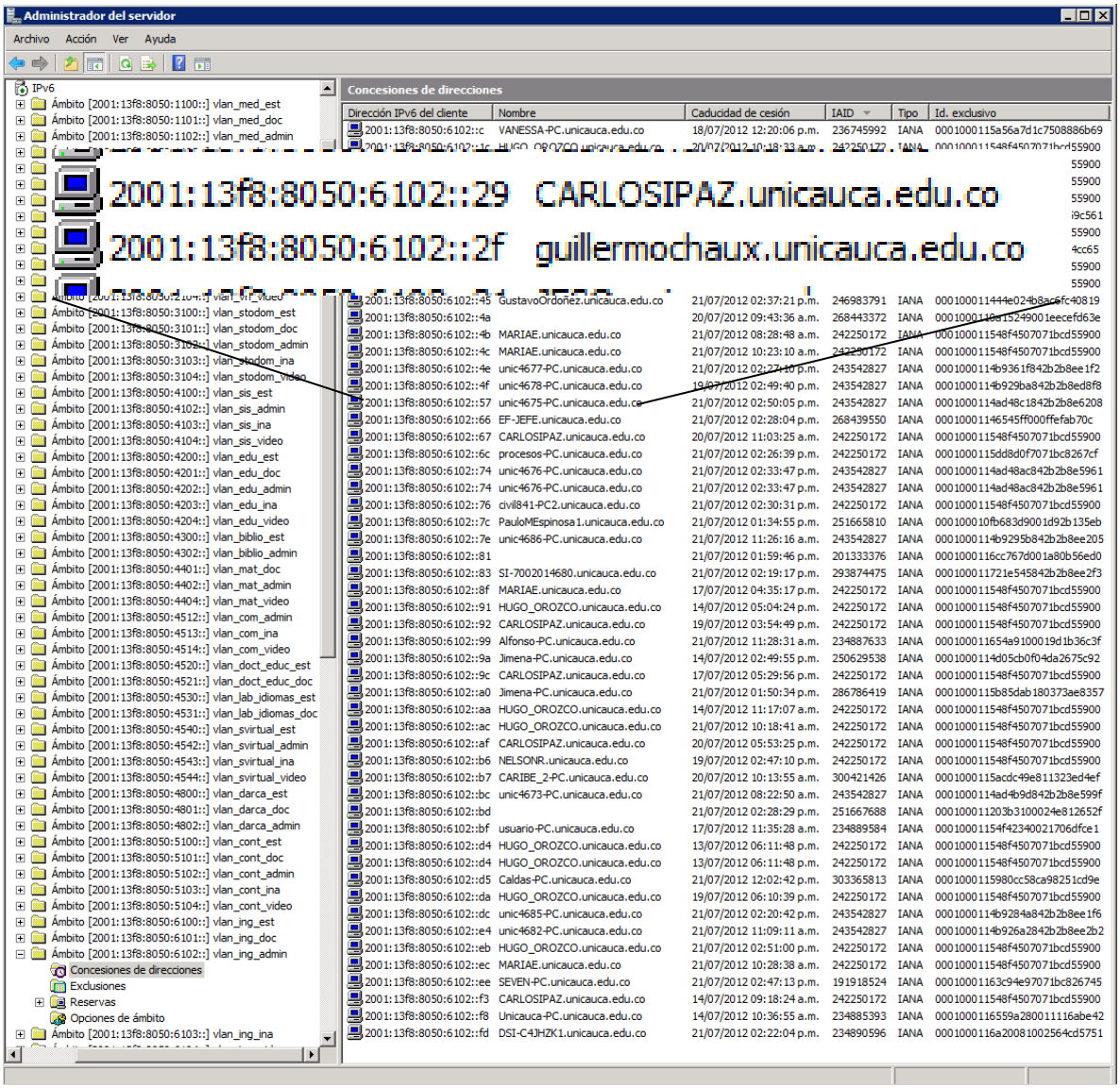

3. Se verifica que después del 06 de Junio de 2012, fecha en que el protocolo IPv6 se hace oficial internacionalmente, se presentan inconvenientes de navegación con los usuarios que hacen uso del servicio NAT en IPv4.

- **Actuar:** se realizan tres ciclos concatenados con la fase de verificar.

1. Como solución al primer ciclo de verificación se lleva a cabo la instalación de un complemento sobre Windows Server lo cual corrige el error con mensajes “Relay”. Como resultado se espera que se asignen correctamente direcciones.

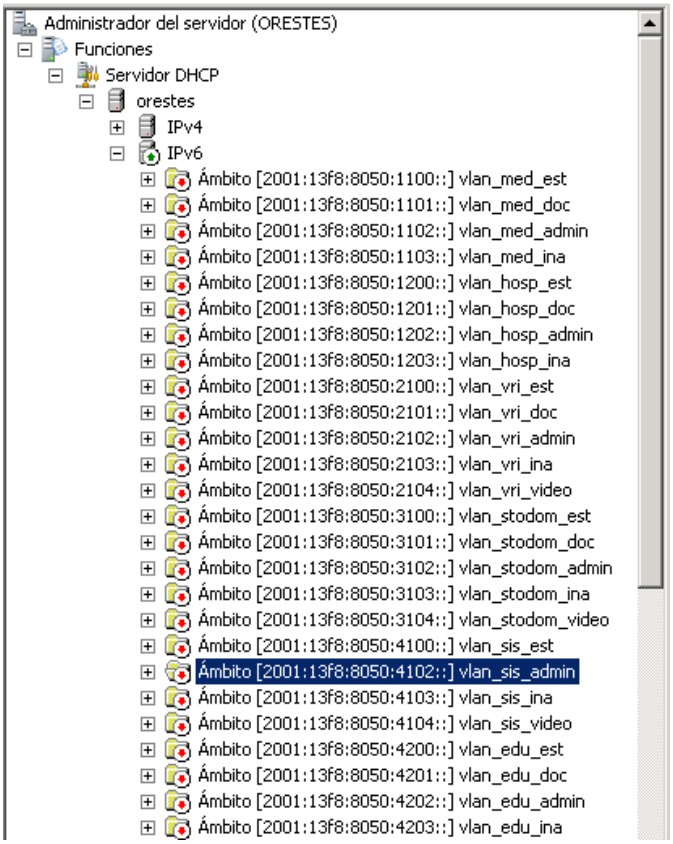
2. Se monitorea la asignación de direcciones.

**Figura 3.1.4 Direcciones Ipv6 asignadas**




3. En respuesta al último ciclo de verificación se procede a deshabilitar todos los ámbitos del servidor DHCPv6, este proceso no implica sacar el servicio de producción como tampoco eliminar dichos ámbitos. La deshabilitación incurre en la pausa de la asignación de direcciones temporalmente. En la Imagen se muestra como el servidor y los ámbitos están desplegados pero desactivados.

**Figura 3.1.5 Servidor DHCP con ámbitos IPv6**

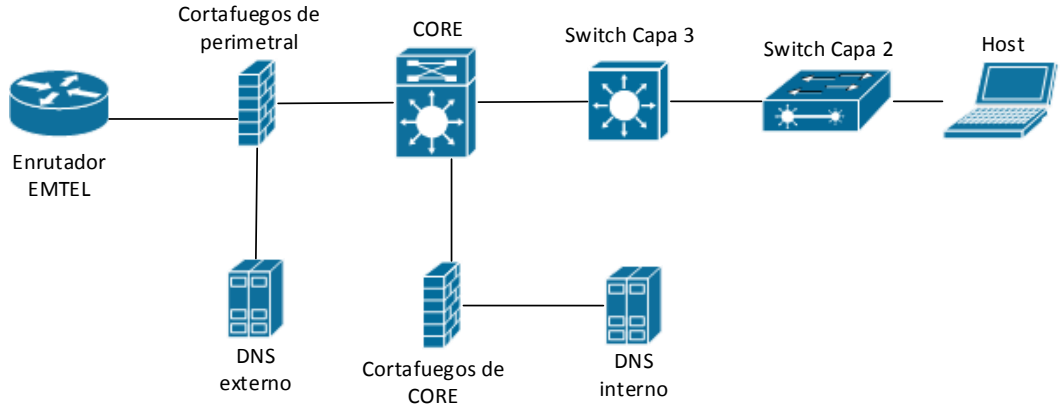



## 3.2 Servicio DNS

En la red de la universidad del Cauca se manejan dos tipos de servidores; los internos que dan la resolución a la Intranet y los externos que dan resolución a Internet. Los primeros, instalados sobre sistemas *Windows Server 2003* SP1 también manejan el Servicio de *Directorio Activo* de *Microsoft Windows*. Estos servidores, Cronos el principal y Hades el secundario, tienen la zona correspondiente al dominio unicauca.edu.co que contiene los registros A, MX y CNAME con direcciones privadas para los servicios que necesiten ser accedidos desde la red interna. Debido a que los usuarios de la LAN también necesitan tener resolución para dominios externos, en estos servidores se configuran los servidores reenviadores para que consulten a los DNS externos Institucionales; dns1 y dns2.

Los DNS externos están instalados sobre servidores Linux de distribución Debian en los cuales también se tiene la zona para el dominio unicauca.edu.co pero en el cual los registros usan direcciones públicas. Estos hacen uso de la aplicación Bind.

**Figura 3.2.1Topologia de red - DNS**




**Sobre Linux:**

- **Planear:** Se tiene como objetivo resolver con registros AAAA las consultas DNS provenientes de la WAN para los dominios *unicauca.edu.co* e *ipv6.unicauca.edu.co.* También debe estar disponible para resolución de consultas desde la Intranet. Estos procesos se deben poder hacer mediante una conexión nativa en el nuevo protocolo. Para iniciar con la implementación se sigue la tabla 3.2.1donde se presenta la información del estado inicial del servicio.

**Tabla 3.2.1 1 Información técnica del servidor DNS, bajo Linux**

| | |
|---|---|
| **Nombre** | DNS1 |
| **Sistema Operativo** | Linux version 2.6.26-2-amd64 (Debian 2.6.32), con GCC version 4.1.3 (Debian 4.1.2-25) |
| **Software** | Bind 9.7.3 |
| **IPv4** | 10.200.1.200 |
| **Registro A** | dns1.unicauca.edu.co |
| | |
| **Nombre** | DNS2 |
| **Sistema Operativo** | Linux version 2.6.26-2-amd64 (Debian 2.6.26-25), con GCC version 4.1.3 (Debian 4.1.2-25) |
| **Software** | Bind 9.7.3 |
| **IPv4** | 10.200.1.201 |
| **Registro A** | dns2.unicauca.edu.co |

Comparando estos datos con los requerimientos mínimos para soporte de IPv6 como se muestra en las tablas 3.2.2 y 3.2.3 se verifica que los servidores soportan IPv6.

**Tabla 3.2.2 Validación del soporte IPv6 sobre el servidor DNS1, bajo Linux**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Linux – Kernel 2.2 o posterior | Debian 4.1.3 – kernel 2.6.32 | Cumple |
| **BIND** | BIND 9 o superior | BIND 9.7.3 | Cumple |

**Tabla 3.2.3 Validación del soporte IPv6 sobre el servidor DNS2, bajo Linux**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Linux – Kernel 2.2 o posterior | Debian 4.1.3 – kernel 2.6.26 | Cumple |
| **BIND** | BIND 9 o superior | BIND 9.7.3 | Cumple |

Una vez establecido el soporte, se aplica el direccionamiento previo, quedando la configuración previa así:

**Tabla 3.2.4 Configuraciones IPv6, previas, para el servidor DNS1, bajo Linux**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| BIND 9.7.3 | Debian 4.1.3 – Linux 2.6.32 | 2001:13f8:8050:f100::3:1 | AAAA: dns1.unicauca.edu.co |

**Tabla 3.2.5 Configuraciones IPv6, previas, para el servidor DNS2, bajo Linux**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| BIND 9.7.3 | Debian 4.1.3 – Linux 2.6.26 | 2001:13f8:8050:f100::3:2 | AAAA: dns2.unicauca.edu.co |

Como parte final de esta fase se deben definir todos los registros AAAA, CNAME y MX que se deben configurar. En la tabla 3.2.6 se resume.

**Tabla 3.2.6 Registros a publicar en DNS**

| Servicio | Registro | Tipo de registro | IPv6 |
|---|---|---|---|
| WEB | unicauca.edu.co | AAAA | 2001:13f8:8050:f110::2 |
| | www.unicauca.edu.co | CNAME | |
| | ipv6.unicauca.edu.co | AAAA | 2001:13f8:8050:f110::2 |
| | www.ipv6.unicauca.edu.co | CNAME | |
| | server.ipv6.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::f1e7:1 |

| | | | |
|---|---|---|---|
| FTP | odin.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::2:1 |
| | ftp.unicauca.edu.co | CNAME | |
| | ftp.ipv6.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::2:1 |
| | ftp6.ipv6.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::f1e7:2 |
| SMTP, POP, IMAP | afrodita.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::5 |
| | afrodita.unicauca.edu.co | MX | |
| | ipv6.afrodita.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::5:1 |
| | ipv6.afrodita.unicauca.edu.co | MX | |
| | mail.owa.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::f1e7:5 |
| | mail.owa.unicauca.edu.co | MX | |

- **Hacer:** Se realiza la configuración de red necesaria para la dirección planeada.

  Debido a que el servicio BIND ya estaba instalado y configurado para soportar la resolución del dominio *unicauca.edu.co sobre IPv4,* se procede a modificar el archivo de configuración de la zona *unicauca* adicionando los registros AAAA planeados para este dominio. En la misma zona se creó el subdominio ipv6 para el cual se asignaron los registros AAAA definidos previamente. Se creó la zona de resolución inversa para 2001:13f8:8050 con todos los punteros necesario para los registros mencionados. El proceso de instalación y configuración se expone más ampliamente en el anexo D1. En la figura 3.2.2 se muestra como queda finalmente. Debido a que los dos servidores se sincronizan automáticamente, la configuración se centra en DNS1 que es el principal.

**Figura 3.2.2 Configuración final de DNS1**

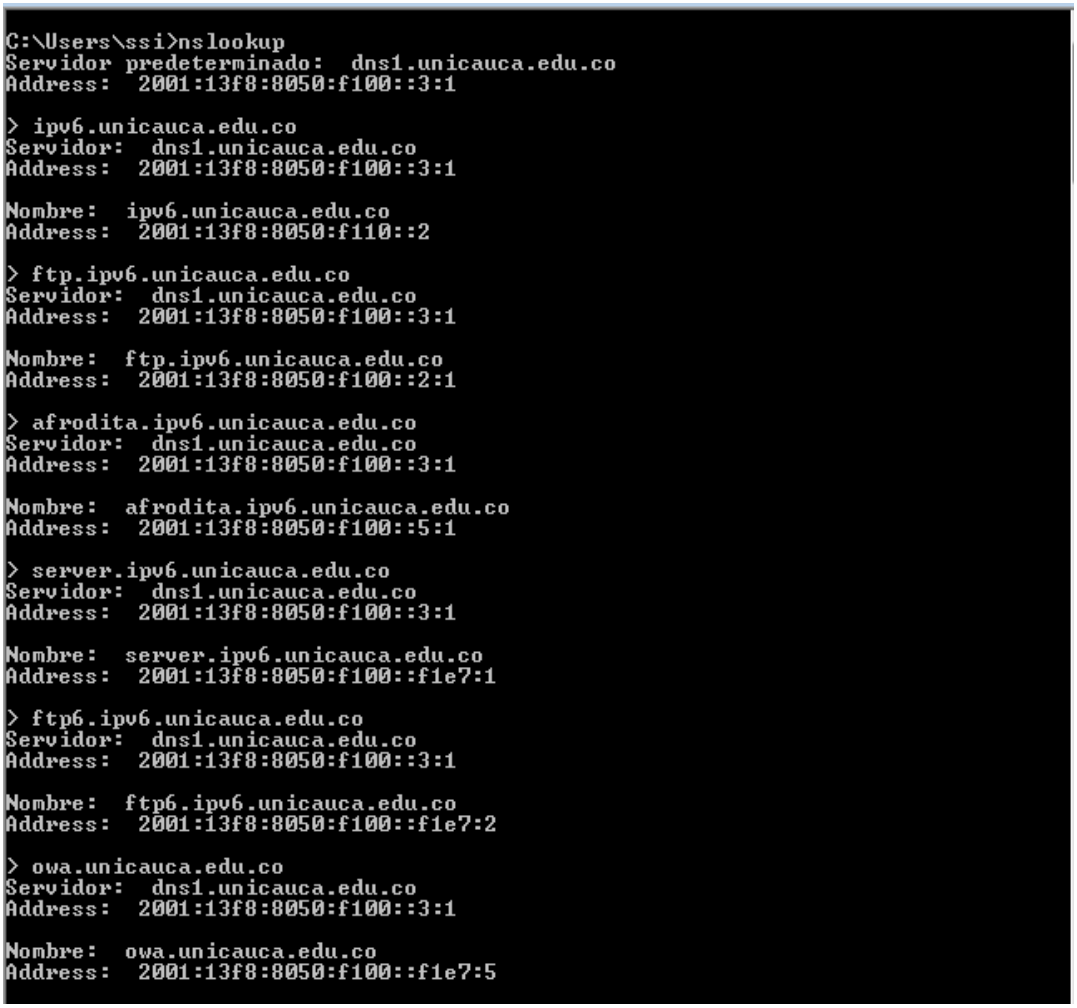
```
 GNU nano 2.2.4          Fichero: /etc/bind/unicauca.edu.co.zone

$ORIGIN ipv6.unicauca.edu.co.

@                       IN      MX      10      afrodita
@                       IN      AAAA            2001:13f8:8050:f110::2
www                     IN      CNAME           ipv6.unicauca.edu.co.
ftp                     IN      AAAA            2001:13f8:8050:f100::2:1
iptv                    IN      AAAA            2001:13f8:8050:4544::c1a:2a
afrodita                IN      AAAA            2001:13f8:8050:f100::5:1
server                  IN      AAAA            2001:13f8:8050:f100::fle7:1
ftp6                    IN      AAAA            2001:13f8:8050:f100::fle7:2


$ORIGIN owa.unicauca.edu.co.

@                       IN      MX      10      mail
@                       IN      AAAA            2001:13f8:8050:f100::fle7:5
mail                    IN      AAAA            2001:13f8:8050:f100::fle7:5
```

- **Verificar:** Esta fase se realiza en dos ciclos en secuencia con la fase de actuar.
  1. Se verifica que la resolución del servidor opera bien sin embargo se prevee que después del dia 06 de Junio de 2012 los registros AAAA de la zona

*unicauca.edu.co* pueden generar inconvenientes en la resolución a consultas provenientes de la WAN, debido a la no publicación de los servicios IPv6 por una red comercial.

**2.** mediante la herramienta "nslookup" que proporciona el sistema operativo Windows se hace una consulta DNS al servidor, la cual debe ser respondida mediante IPv6. Para cada registro publicado se hace una consulta las cuales se muestran en la figura 3.2.3.

**Figura 3.2.3 Consultas DNS a servidor DNS1**




- **Actuar:** En esta fase se da respuesta al primer ciclo de la fase anterior mediante la eliminación de los registros AAAA para la zona principal de la Universidad. Sin embargo el subdominio *ipv6.unicauca.edu.co* queda publicado con todas las resoluciones previas como se muestra en la tabla 3.2.7.

**Tabla 3.2.7 Registros publicados en DNS y DNS2**

| Servicio | Registro | Tipo de registro | IPv6 |
|---|---|---|---|
| WEB | ipv6.unicauca.edu.co | AAAA | 2001:13f8:8050:f110::2 |
| | www.ipv6.unicauca.edu.co | CNAME | |
| | server.ipv6.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::f1e7:1 |
| FTP | ftp.ipv6.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::2:1 |
| | ftp6.ipv6.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::f1e7:2 |
| SMTP, POP, IMAP | ipv6.afrodita.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::5:1 |
| | ipv6.afrodita.unicauca.edu.co | MX | |
| | mail.owa.unicauca.edu.co | AAAA | 2001:13f8:8050:f100::f1e7:5 |
| | mail.owa.unicauca.edu.co | MX | |

**Sobre Windows Server:**

- **Planear:** El objetivo de esta implementación es dar resolución con registros AAAA a las consultas DNS provenientes de la Intranet para los dominios *unicauca.edu.co* e *ipv6.unicauca.edu.co*. Para iniciar con la implementación se sigue la tabla 3.2.8 donde se presenta la información del estado inicial del servicio.

**Tabla 3.2.8 Información técnica del servidor DNS, bajo Windows Server**

| | |
|---|---|
| **Nombre** | Cronos |
| **Sistema Operativo** | Windows Server 2003 |
| **Software** | Aplicación Nativa |
| **IPv4** | 172.16.255.200 |
| **Registro A** | cronos.unicauca.edu.co |
| | |
| **Nombre** | Hades |
| **Sistema Operativo** | Windows Server 2003 |
| **Software** | Aplicación Nativa |
| **IPv4** | 172.16.255.183 |
| **Registro A** | hades.unicauca.edu.co |

Comparando estos datos con los requerimientos mínimos para soporte de IPv6 como se muestra en las tablas 3.2.9 y 3.2.10 se verifica que los servidores no soportan IPv6.

**Tabla 3.2.9 Validación del soporte IPv6 sobre el servidor Cronos, Windows Server**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Windows Server 2008 o posterior | Windows Server 2003 SP2 | No cumple |
| **DNS** | Nativo | ---------- | ---------- |

**Tabla 3.2.10 Validación del soporte IPv6 sobre el servidor Hades, bajo Windows Server**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Windows Server 2008 o posterior | Windows Server 2003 SP2 | No cumple |
| **DNS** | Nativo | ---------- | ---------- |

Debido a la no compatibilidad del protocolo sobre los servidores se debe llevar a cabo la siguiente lista de actividades para poder desplegar las configuraciones del nuevo protocolo:

1. Instalación de un nuevo servidor con sistema operativo Windows Server 2008 con una IP cualquiera. Llevarlo a un punto estable con las últimas actualizaciones.
2. Adición de este servidor al directorio activo, de esta manera puede obtener todas las zonas publicadas en los servidores originales.
3. Una vez ha copiado las zonas, se promueve a administrador del Directorio Activo y se procede a desconectar el servidor antiguo
4. Finalmente se configura la IP (172.16.255.200) con la que se publica el servicio DNS.

Para la actualización del servidor secundario se siguen los pasos 1 y 2, de esta manera se mantiene sincronizado con el principal.

En esta instancia se tienen los servidores dispuestos para implementar IPv6 partir del direccionamiento previo. Las configuraciones previas se muestran en la tabla 3.2.11 y 3.2.12.

**Tabla 3.2.11 Configuraciones IPv6, previas, para el servidor Cronos, bajo Windows Server**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| DNS | Windows server 2008 SP2 | 2001:13f8:8050:f230::1:1 | AAAA: cronos.unicauca.edu.co |

**Tabla 3.2.12 Configuraciones IPv6, previas, para el servidor Hades, bajo Windows Server**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| DNS | Windows server 2008 SP2 | 2001:13f8:8050:f230::1:2 | AAAA: hades.unicauca.edu.co |

Para la configuración de registros que se deben publicar se sigue la tabla 3.2.6 vista previamente.

- **Hacer:** Se realiza la configuración de la interfaz de red y se procede con el anexo D.2 para el despliegue de zonas para IPv6. Para llevar a cabo la publicación de los dominios *unicauca.edu.co* e *ipv6.unicauca.edu.co* se agregan los registros mencionados en la fase anterior, en las figuras 3.2.4 3.2.5 se muestra el estado final del servidor.

**Figura 3.2.4 Zona *unicauca.edu.co* en Windows Server**

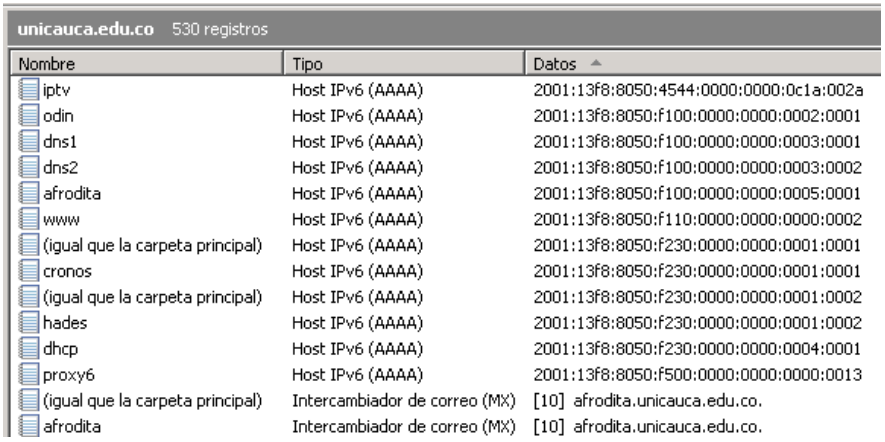
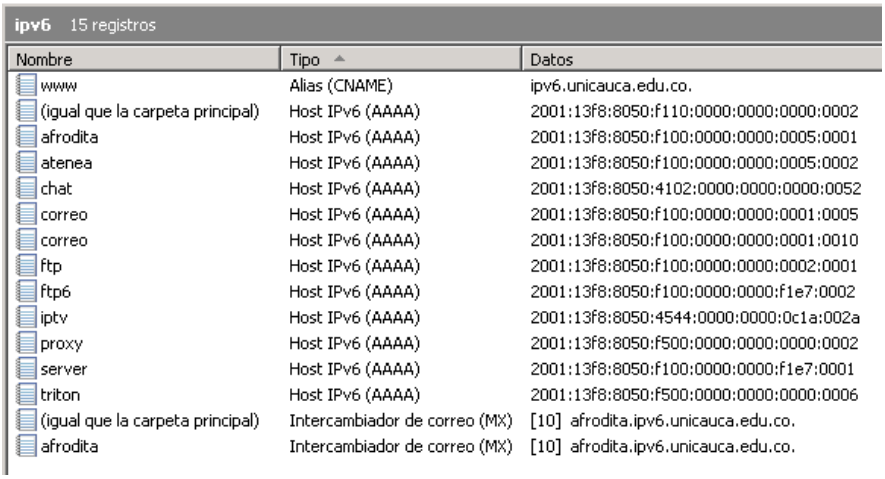


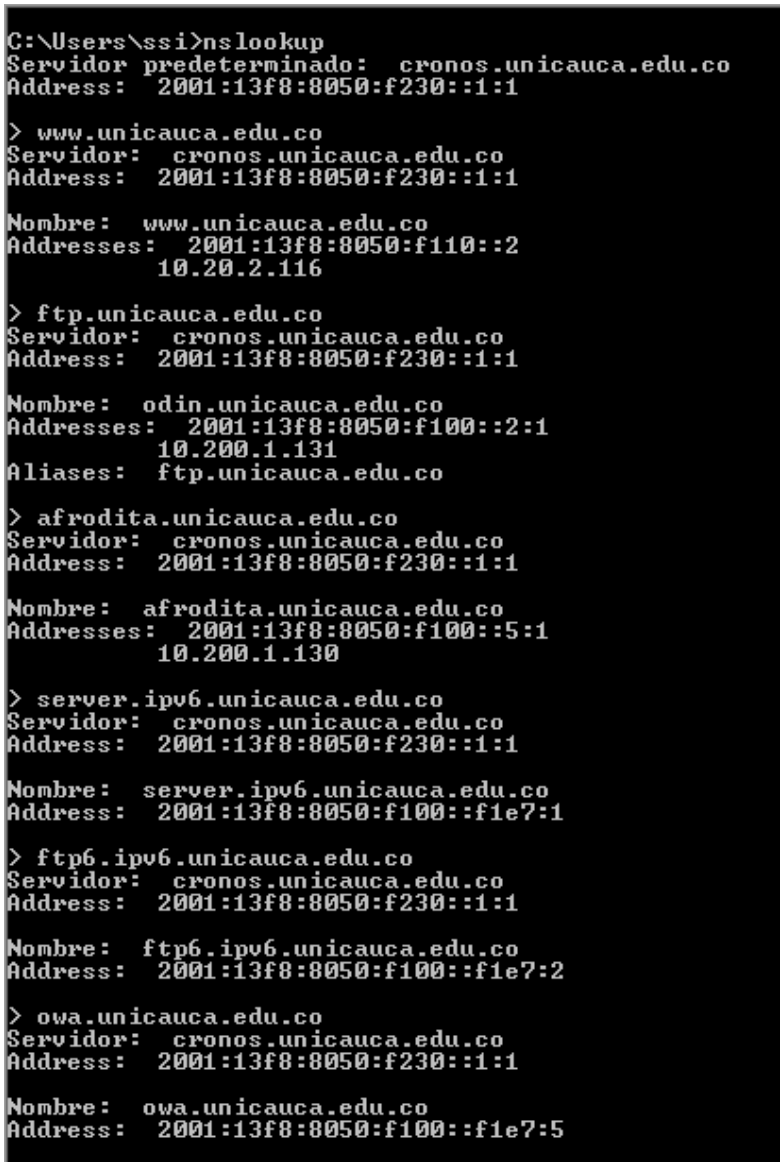

**Figura 3.2.5 Zona ipv6.unicauca.edu.co en Windows Server**



Dado que los servidores de la intranet también deben proveer resolución de registros de internet, se configura en estos dos servidores la opción de reenviadores para que consulten a los externos de la Institución, lo que permite que una consulta de un dominio externo sea dirigida a los dos servidores Linux que tienen salida a internet.

- **Verificar:** mediante el mismo procedimiento de la verificación realizada sobre Linux, se tiene en un equipo la resolución mostrada en la imagen 3.2.5.

**Figura 3.2.6 Consultas DNS a servidor Cronos**

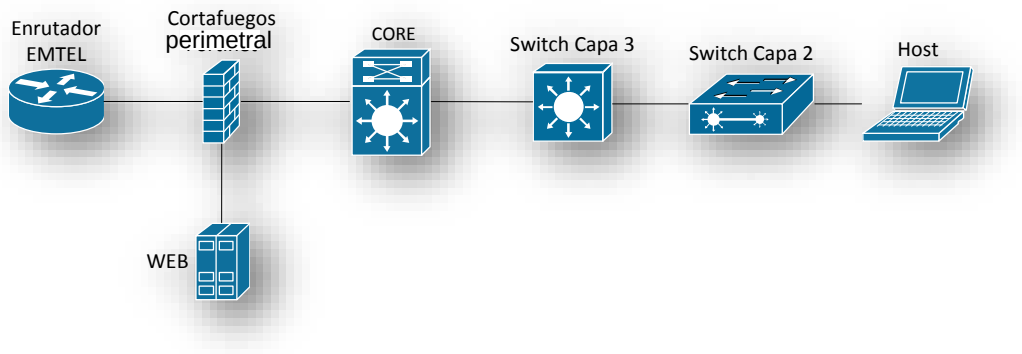


## 3.3 Servicio WEB

Se tiene como objetivo la implementación del Protocolo IPv6 sobre una página WEB de la Institución el cual está sobre un servidor con sistema operativo Linux, para el servicio sobre Windows Server se toma un nuevo servidor sobre el cual se despliega una copia del mencionado anteriormente.

De la fase de diseño de red se tiene la siguiente topología para acceso al servicio WEB.

**Figura 3.3.1 Acceso a servicios WEB IPv6**




**Sobre Linux:**

- **Planear:** El objetivo es brindar acceso WEB por IPv6 al portal de la Institución que se encuentra en producción en IPv4. Se parte de un servidor con unas características resumidas en la tabla 3.3.1.

**Tabla 3.3.1 Información técnica del servidor WEB, bajo Linux**

| | |
|---|---|
| **Nombre** | balanceadorExt |
| **Sistema Operativo** | Linux version 2.6.26-2-amd64 (Debian 2.6.26-25), con GCC version 4.1.3 (Debian 4.1.2-25) |
| **Software** | Apache – versión 2.2.9 |
| **IPv4** | 10.20.3.116 |
| **Registro A** | www.unicauca.edu.co |

De acuerdo a esta tabla no es necesaria la reinstalación o actualización del sistema operativo ni del software que se utiliza para el servicio WEB. En la tabla 3.3.2 se expone la versión requerida y usada para cada uno.

**Tabla 3.3.2 Validación del soporte IPv6 sobre el servidor WEB, bajo Linux**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Linux – Kernel 2.2 o posterior | Debian 4.1.3 – kernel 2.6.26 | Cumple |
| **Apache** | Apache 2.0 o posterior | 2.2.9 | Cumple |

De acuerdo al plan de direccionamiento planteado, en la sección 2.2.2, se define que la dirección IPv6 a configurar sobre la interfaz del servidor será 2001:13f8:8050:f110::2, *ipv6.unicauca.edu.co* será el registro AAAA, que se creará sobre el DNS. Esta información se resume en la tabla 3.3.3

**Tabla 3.3.3 Configuraciones IPv6, previas, para el servidor WEB, bajo Linux**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| WEB Apache 2.2.9 | Debian 4.1.3 – Linux 2.6.26 | 2001:13f8:8050:f110::2 | AAAA: ipv6.unicauca.edu.co<br>CNAME: www.ipv6.unicauca.edu.co |

- **Hacer:** se configura la interfaz de red del servidor con la dirección IPv6 planeada y reinicia el servicio de red mediante el módulo *networking*, este proceso se explica mejor en el anexo XXXX de manera general para los servidores sobre Linux. Posteriormente se procede con la configuración del servicio como se muestra en el Anexo E.1.

- **Verificar:** para comprobar que el servidor está estableciendo sesiones en IPv6 por el puerto 80 se utiliza el comando “netstat -tan |grep :: |grep 80” el cual muestra sesiones establecidas como lo muestra la figura 3.3.2.

**Figura 3.3.2 Verificación de puertos en Servidor WEB Linux**

```
balanceadorExt:~# netstat -tan |grep :: |grep 80
tcp6       0      0 :::80                   :::*                    LISTEN
tcp6       0      0 2001:13f8:8050:f110::80 2001:13f8:8050:41:49361 TIME_WAIT
tcp6       0      0 2001:13f8:8050:f110::80 2001:13f8:8050:41:49360 TIME_WAIT
tcp6       0      0 2001:13f8:8050:f110::80 2001:13f8:8050:41:49359 TIME_WAIT
```

- **Actuar:** Finalmente, para publicar el servicio se configuran los registros AAAA y CNAME planeados tanto en los servidores internos como externos de la Institución.

Una vez cumplidos estos pasos se tiene accesible para los usuarios el servicio WEB IPv6 sobre Linux como se muestra en las figuras 3.3.3 y 3.3.4 en donde se accede desde el equipo con IPv6 “2001:13f8:8050:4102::a” mediante un navegador WEB y se verifica el establecimiento de la sesión con el comando “netstat -a -n -p tcpv6”.

**Figura 3.3.3 Sesiones cliente-servidor Linux en IPv6**

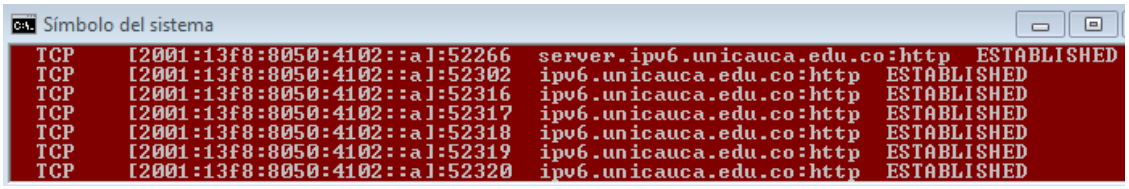



**Figura 3.3.4 Pagina WEB en Windows Server accedida por IPv6**


**Sobre Windows Server:**

- **Planear:** El objetivo, es brindar el servicio WEB Institucional, a través de IPv6 sobre el servidor WEB de la Universidad del Cauca, el cual, cuenta con un sistema operativo Windows Server 2008 Service Pack 2, bajo el software IIS (*Internet Information Server*) versión 7.0. En la tabla 3.3.4, se resume la información del servidor.

**Tabla 3.3.4 Información técnica del servidor WEB, bajo Windows Server**

| | |
|---|---|
| **Nombre** | FTP-WEB |
| **Sistema Operativo** | Windows Server 2008 Service Pack 2 |
| **Versión IIS** | 7.0 |
| **IPv4** | 10.200.1.39 |

De acuerdo a la información anterior, no es necesario realizar actualizaciones sobre el Sistema Operativo, ni para el Software IIS 7.0, para soportar IPv6, ya que como se indica en la tabla 3.3.5, se cumple con las condiciones.

**Tabla 3.3.5 Validación del soporte IPv6 sobre el servidor WEB, bajo Windows Server 2008**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Para Windows Server 2008, IPv6 se encuentra activado de manera predeterminada. Teredo se encuentra habilitado por defecto, pero permanece inactivo hasta que una aplicación o servicio intenta usarlo [25] | Windows Server 2008 | Cumple |
| **IIS** | Soporta IPv6 desde la versión 6.0 [26] | 7.0 | Cumple |

De acuerdo al plan de direccionamiento planteado, en la sección 2.2.2, se define que la dirección IPv6 a configurar sobre la interfaz del servidor WEB, será 2001:13f8:8050:f100::f1e7:1 y server.ipv6.unicauca.edu.co será el registro AAAA, que se creará sobre el DNS. Esta información se resume en la tabla 3.3.6.

**Tabla 3.3.6 Configuraciones IPv6, previas, para el servidor WEB, bajo Windows Server 2008**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| IIS | Windows Server 2008 | 2001:13f8:8050:f100::f1e7:1 | server.ipv6.unicauca.edu.co |
| Servicio de Publicación FTP | | | |

- **Hacer:** Se instaló un contenedor con las especificaciones mencionadas en la tabla 3.3.7, en la cual se configuró la dirección IPv6 y se instaló IIS, agregando las características que soportan el servicio WEB.

  Se agrega un sitio WEB, y se asocia las direcciones IPv6 dentro de la configuración del servicio, para permitir las conexiones, a través de este protocolo.

**Tabla 3.3.7 Pasos realizados para la configuración del servicio WEB con soporte IPv6, bajo Windows Server 2008**

| Paso | Acción |
|---|---|
| 1 | Adecuación del contenedor |
| 2 | Instalación de IIS 7.0 |
| 3 | Agregar un sitio WEB |
| 4 | Configurar el servicio WEB para escuchar conexiones a través de direcciones IPv6. |

- **Verificar:** Para comprobar que el servidor está escuchando por el puerto 80, a través de IPv6, se puede utilizar el comando ***netstat –a –n –p tcpv6***

- **Actuar:** Finalmente, para facilitar el acceso a los usuarios, se configura el registro AAAA sobre el DNS interno, dentro del dominio IPv6 y de esta forma acceder al servicio, a través de server.ipv6.unicauca.edu.co.

  Como medida de seguridad, se crean políticas en el cortafuegos, en el que solo se permiten acceso a la IP 2001:13f8:8050:f100::f1e7:1, a través del puerto 80, para permitir el acceso al WEB.

En las figuras 3.3.5 y 3.3.6, se evidencia el establecimiento de la conexión al servicio WEB, a través del protocolo IPv6

**Figura 3.3.5 Sesiones cliente-servidor Windows en IPv6**

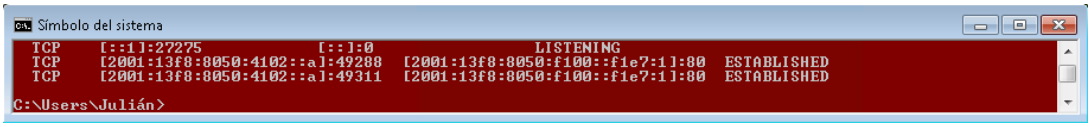


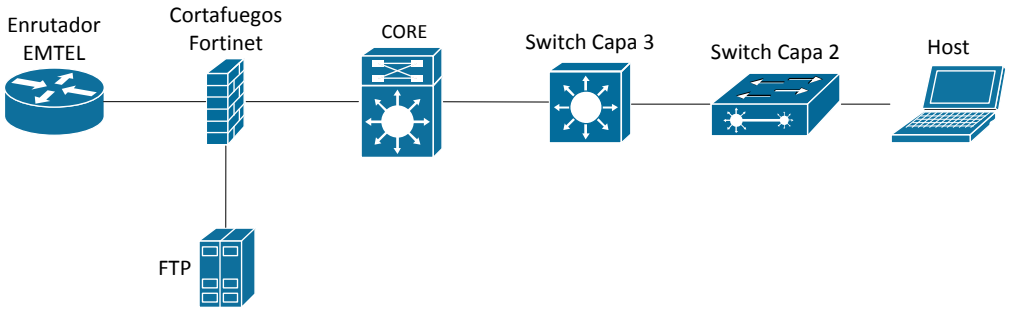

**Figura 3.3.6 Pagina WEB en Linux accedida por IPv6**

## 3.4 Servicio FTP.

Se tiene como objetivo, la implementación de Protocolo IPv6 sobre el servidor de FTP, contando con el servicio Vsftpd, ya instalado sobre la VLAN 60 y la instalación y configuración de un servidor Windows Server con IIS sobre la VLAN 80.

En la figura 3.4.1, se identifica la ubicación del servidor FTP, dentro de la red de información de la Universidad del Cauca.

**Figura 3.4.1 Topología de red - FTP**




**Sobre Linux:**

- **Planear:** El objetivo es brindar el servicio FTP Institucional, a través de IPv6 sobre el servidor FTP de la Universidad del Cauca, el cual, cuenta con un sistema operativo Linux versión 2.6.32-5-686 (Debian 2.6.32-48squeeze1), con GCC versión 4.3.5 (Debian 4.3.5-4), bajo el software vsFTPd 2.3.2. En la tabla 3.4.1, se resume la información del servidor.

**Tabla 3.4.1 Información técnica del servidor FTP, bajo Linux Debian**

| | |
|---|---|
| **Nombre** | Odin |
| **Sistema Operativo** | Linux versión 2.6.32-5-686 (Debian 2.6.32-48squeeze1), con GCC versión 4.3.5 (Debian 4.3.5-4) |
| **Versión vsFTPd** | 2.3.2 |
| **IPv4** | 10.200.1.131 |
| **Registro A** | ftp.unicauca.edu.co |

De acuerdo a la información anterior, no es necesario realizar actualizaciones sobre el Sistema Operativo, ni sobre el Software vsFTPd para soportar IPv6, ya que como se indica en la tabla 3.4.2, se cumple con las condiciones.

**Tabla 3.4.2 Validación del soporte IPv6 sobre el servidor FTP , bajo Linux Debian**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Distribuciones con kernel superior a 2.2.x | 2.6.32-5-686 | Cumple |
| **vsFTPd** | 2.x | 2.3.2 | Cumple |

De acuerdo al plan de direccionamiento planteado, en la sección 2.2.2, se define que la dirección IPv6 a configurar sobre la interfaz del servidor FTP será 2001:13f8:8050:f100::2:1 y ftp.ipv6.unicauca.edu.co será el registro AAAA, que se creará sobre el DNS. Esta información se resume en la tabla 3.4.3.

**Tabla 3.4.3 Configuraciones IPv6, previas, para el servidor FTP, bajo Linux Debian**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| vsFTPd | Linux | 2001:13f8:8050:f100::2:1 | ftp.ipv6.unicauca.edu.co |

- **Hacer:** Se instaló una maquina virtual, con las mismas versiones de Linux y vsFTPd del ambiente de producción, en la cual se configuró una dirección IPv6 y se editó el archivo de configuración de vsFTPd para habilitar el soporte IPv6 sobre este servicio.

  Se modifica el archivo de configuración, ubicado en la ruta: /etc/vsftpd.conf, para habilitar el soporte IPv6 en vsFTPd, declarando la directiva ***listen*** como se indica a continuación:

  ```
  listen=NO
  listen_ipv6=YES
  ```

  Para hacer efectivos los cambios se reinicia el servicio ejecutando ***service vsftpd restart.*** En la tabla 3.4.4, se resume los pasos realizados en esta etapa.

**Tabla 3.4.4 Pasos realizados para la configuración del servicio FTP con soporte IPv6, bajo Linux Debian**

| Paso | Acción |
|---|---|
| 1 | Adecuación del ambiente de pruebas. |
| 2 | Modificación del archivo de configuración de vsFTPd |
| 3 | Reinicio del servicio para hacer efectivo los cambios |

- **Verificar:** Para comprobar que está escuchando por IPv6 el servidor en el puerto 21 se puede utilizar el comando ***netstat –tan***

Una vez comprobado el correcto funcionamiento del servicio FTP, a través de IPv6, se procede a notificar al Ing. De SSI, para que los cambios sean aplicados sobre el servidor de producción.

- **Actuar:** Finalmente, para facilitar el acceso a los usuarios, se configura el registro AAAA sobre el DNS interno, dentro del dominio IPv6 y de esta forma acceder al servicio, a través de ftp.ipv6.unicauca.edu.co.

  Como medida de seguridad, se crean políticas en el cortafuegos, en el que solo se permiten acceso a la IP 2001:13f8:8050:f100::2:1, a través del puerto 20 y 21, para permitir el acceso al FTP, como también al puerto 80, para permitir el acceso, a través de la WEB.

  En la figura 3.4.2, se evidencia el funcionamiento del servicio FTP, sobre Linux.

**Figura 3.4.2 Verificación del servicio FTP sobre Linux**


**Sobre Windows Server:**

- **Planear:** El objetivo es brindar el servicio FTP Institucional a través de IPv6 sobre el servidor FTP de la Universidad del Cauca, el cual cuenta con un sistema operativo Windows Server 2008 Service Pack 2, bajo el software IIS versión 7.0 (*Internet Information Server*) y Servicio de publicación FTP versión 7.5 . En la tabla 3.4.5, se resume la información del servidor.

**Tabla 3.4.5 Información técnica del servidor FTP, bajo Windows Server 2008**

| | |
|---|---|
| **Nombre** | FTP-WEB |
| **Sistema Operativo** | Windows Server 2008 Service Pack 2 |
| **Versión IIS** | 7.0 |
| **Versión Servicio de Publicación FTP** | 7.5 |
| **IPv4** | 10.200.1.39 |

De acuerdo a la información anterior, no es necesario realizar actualizaciones sobre el Sistema Operativo, ni para los Software IIS 7.0 y Servicio de Publicación FTP 7.5 para soportar IPv6, ya que como se indica en la tabla 3.4.6, se cumple con las condiciones.

**Tabla 3.4.6 Validación del soporte IPv6 sobre el servidor FTP, bajo Windows Server 2008**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Para Windows Server 2008, IPv6 se encuentra activado de manera predeterminada. Teredo se encuentra habilitado por defecto, pero permanece inactivo hasta que una aplicación o servicio intenta usarlo [25] | Windows Server 2008 | Cumple |
| **IIS** | Soporta IPv6 desde la versión 6.0 [26] | 7.0 | Cumple |
| **Servicio de Publicación FTP** | Soporte IPv6 desde la versión 7.0 [27] | 7.5 | Cumple |

De acuerdo al plan de direccionamiento planteado, en la sección 2.2.2, se define que la dirección IPv6 a configurar sobre la interfaz del servidor FTP será 2001:13f8:8050:f100::f1e7:2 y ftp6.ipv6.unicauca.edu.co será el registro AAAA, que se creará sobre el DNS. Esta información se resume en la tabla 3.4.7.

**Tabla 3.4.7 Configuraciones IPv6, previas, para el servidor FTP, bajo Windows Server 2008**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| IIS<br>Servicio de Publicación FTP | Windows Server 2008 | 2001:13f8:8050:f100::f1e7:2 | ftp6.ipv6.unicauca.edu.co |

- **Hacer:** Se instalo un contenedor con las especificaciones mencionadas en la tabla 3.4.6, en la cual se configuró la dirección IPv6 y se instaló IIS, agregando la característica Servicio de Publicación FTP.

Se agrega un sitio FTP, y se asocia las direcciones IPv6 dentro de la configuración del servicio, para permitir las conexiones a través de este protocolo.

**Tabla 3.4.8 Pasos realizados para la configuración del servicio FTP con soporte IPv6, bajo Windows Server 2008**

| Paso | Acción |
|---|---|
| 1 | Adecuación del contenedor (Sistema Operativo y Red) |
| 2 | Instalación de IIS 7.0 |
| 3 | Instalación del Servidor de Publicaciones FTP 7.5 |
| 4 | Configurar el servicio FTP para escuchar conexiones a través de direcciones IPv6. |

- **Verificar:** Para comprobar que está escuchando por IPv6 el servidor en el puerto 21 se puede utilizar el comando ***netstat –a –n –p tcpv6***

- **Actuar:** Finalmente, para facilitar el acceso a los usuarios, se configura el registro AAAA sobre el DNS interno, dentro del dominio IPv6 y de esta forma acceder al servicio, a través de ftp6.ipv6.unicauca.edu.co.

  Como medida de seguridad, se crean políticas en el cortafuegos, en el que solo se permiten acceso a la IP 2001:13f8:8050:f100::f1e7:2, a través del puerto 20 y 21, para permitir el acceso al FTP, como también al puerto 80, para permitir el acceso, a través de la WEB.

  En la figura 3.4.3, se evidencia los puertos 21 y 80, escuchando a través de IPv6, como también el acceso al FTP.

**Figura 3.4.3 Verificación del servicio FTP sobre Windows Server**

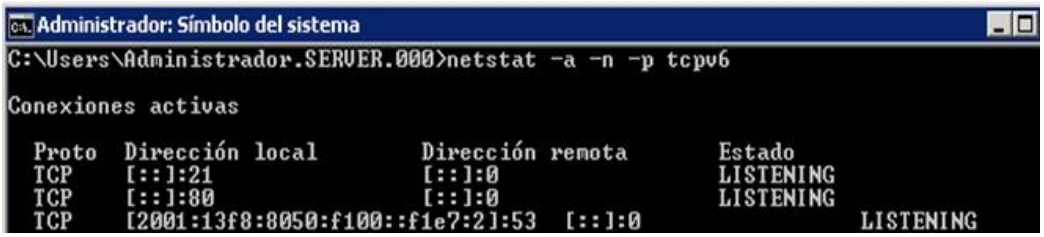
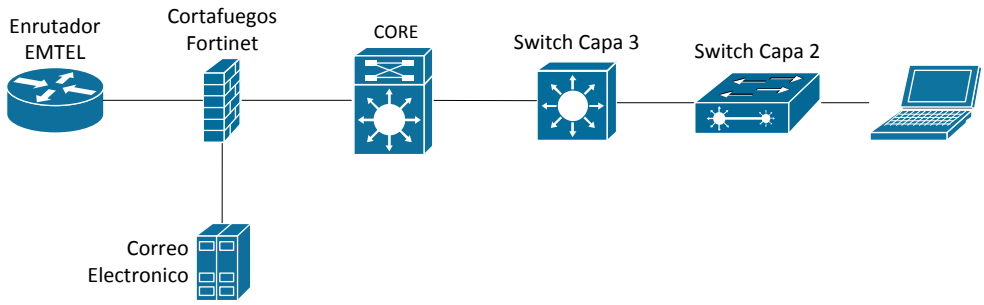


**Figura 3.4.4 Servicio FTP en navegador**


## 3.5 Servicio E-mail

En la figura 3.5.1, se identifica la ubicación del servidor Correo dentro de la red de información de la Universidad del Cauca.

**Figura 3.5.1 Topología de red - E-mail**




**Sobre Linux:**

- **Planear:** El objetivo es brindar el servicio de Correo Institucional a través de IPv6 sobre el servidor Correo de la Universidad del Cauca, el cual cuenta con un sistema operativo Linux versión 2.6.32-5-amd64 (Debian 2.6.32-41squeeze2) (gcc versión 4.3.5 (Debian 4.3.5-4)), y se hace uso de Dovecot 2.0.16, para el correo entrante y Postfix 2.7.1, para el correo saliente. En la tabla 3.5.1, se resume la información del servidor.

**Tabla 3.5.1 Información técnica del servidor Correo, bajo Linux Debian**

| | |
|---|---|
| **Nombre** | Afrodita |
| **Sistema Operativo** | Linux versión 2.6.32-5-amd64 (Debian 5 squeeze2) |
| **Dovecot** | 2.0.16 |
| **Postfix** | 2.7.1 |
| **IPv4** | 10.200.1.130 |
| **Registro A** | afrodita.unicauca.edu.co |

De acuerdo a la información anterior, no es necesario realizar actualizaciones sobre el Sistema Operativo, ni sobre los Software Dovecot y Postfix para soportar IPv6, ya que como se indica en la tabla 3.5.2, se cumple con las condiciones.

**Tabla 3.5.2 Validación del soporte IPv6 sobre el servidor Correo, bajo Linux Debian**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Distribuciones con kernel superior a 2.2.x | 2.6.32-5-686 | Cumple |
| **Dovecot** | 1.x [29] | 2.0.16 | Cumple |
| **Postfix** | 2.2 [28] | 2.7.1 | Cumple |

De acuerdo al plan de direccionamiento planteado, en la sección 2.2.2, se define que la dirección IPv6 a configurar sobre la interfaz del servidor Correo será 2001:13f8:8050:f100::5:1 y afrodita.ipv6.unicauca.edu.co será el registro AAAA, que se creará sobre el DNS. Esta información se resume en la tabla 3.5.3.

**Tabla 3.5.3 Configuraciones IPv6, previas, para el servidor Correo, bajo Linux Debian**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| Dovecot | Linux | 2001:13f8:8050:f100::5:1 | afrodita.ipv6.unicauca.edu.co |
| Postfix | | | |

- **Hacer:** Se instaló una maquina virtual, con las mismas versiones de Linux, Dovecot y Postfix del ambiente de producción, en la cual se configuró una dirección IPv6 y se editaron los respectivos archivos de configuración para los servicios de salida y entrada de correos.

  Para el servicio de salida Postfix, se modifica el archivo de configuración, ubicado en la ruta: /etc/postfix/main.cf, modificando las siguientes directivas:

  - Para habilitar el soporte IPv6 en Postfix se incluye:
    inet_protocols = all // IPv4 e IPv6 si esta activo en el sistema operativo
    inet_protocols = ipv4, ipv6 //IPv4 e IPv6
    inet_protocols = ipv6 // Solo IPv6
    inet_protocols = ipv4 // Solo IPv4

  - Cuando se tiene un servidor con varias interfaces configuradas con IPv6, la directiva que permite indicar que dirección IPv6 se usara para la entrega de correo es:
    smtp_bind_address6 = 2001:13f8:8050:e100::fffe

- Para indicar host y redes confiables que pueden enviar y recibir correos a través del servidor SMTP:
  mynetworks = 127.0.0.0/8 192.168.0.0/16 [::ffff:127.0.0.0]/104 [::1]/128 [2001:13f8:8050::]/64 [fe80::]/64 // Importante que las direcciones IPv6 estén definidas dentro de "[]"

- Como configuraciones adicionales se tiene:
  mydomain = ipv6.unicauca.edu.co
  myhostname = servicios.ipv6.unicauca.edu.co
  myorigin = $mydomain
  mydestination = ipv6.unicauca.edu.co , servicios.ipv6.unicauca.edu.co, localhost.localdomain, localhost

Para hacer efectivos los cambios se reinicia el servicio ejecutando ***service postfix restart.*** En la tabla 3.5.4, se resume los pasos realizados en esta etapa.

**Tabla 3.55.4 Pasos realizados para la configuración del servicio Correo entrante con soporte IPv6, bajo Linux Debian**

| Paso | Acción |
|---|---|
| 1 | Adecuación del ambiente de pruebas. |
| 2 | Modificación del archivo de configuración de Postfix |
| 3 | Reinicio del servicio para hacer efectivo los cambios |

Para el servicio de salida Dovecot, se modifica el archivo de configuración, ubicado en la ruta: /etc/dovecot/dovecot.cf, modificando las siguientes directivas:

listen = [::] //Para escuchar por IPv6
listen = *, [::] //Para escuchar por IPv4 e IPv6
listen = * //Para escuchar por IPv4

Para hacer efectivos los cambios se reinicia el servicio ejecutando ***service dovecot restart.*** En la tabla 3.5.5, se resume los pasos realizados en esta etapa.

**Tabla 3.5.4 Pasos realizados para la configuración del servicio Correo saliente con soporte IPv6, bajo Linux Debian**

| Paso | Acción |
|---|---|
| 1 | Adecuación del ambiente de pruebas. |
| 2 | Modificación del archivo de configuración de Dovecot |
| 3 | Reinicio del servicio para hacer efectivo los cambios |

- **Verificar:** Se realizan validaciones de envío y recepción de correo desde clientes con IPv6 revisando que en la cabecera del mensaje aparezcan relacionada la

dirección IPv6 del servidor indicando que la conexión se estableció a través del nuevo protocolo.

Para comprobar que está escuchando por IPv6 el servidor en el puerto 25, 110 y 143 se puede utilizar el comando ***netstat –tan***

Una vez comprobado el correcto funcionamiento del servicio Correo, a través de IPv6, se procede a notificar al Ing. De SSI, para que los cambios sean aplicados sobre el servidor de producción.

- **Actuar:** Finalmente, para facilitar el acceso a los usuarios, se configura el registro AAAA sobre el DNS interno, dentro del dominio IPv6 y de esta forma acceder al servicio, a través de afrodita.ipv6.unicauca.edu.co.

  Como medida de seguridad, se crean políticas en el cortafuegos, en el que solo se permiten acceso a la IP 2001:13f8:8050:f100::5:1, a través del puerto 25, 110 y 143, para permitir el Servicio de entrada y salida de correos. En la figura 3.5.2, se evidencia el funcionamiento del servicio Correo, sobre Linux.

**Figura 3.5.2 Verificación del servicio Correo sobre Linux**

```
[root@linux ~]# netstat -tanpul
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
...
tcp        0      0 :::25                       :::*                        LISTEN      15865/master
```

```
[root@linux ~]# netstat -tanpul
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address               Foreign Address             State       PID/Program name
...
tcp        0      0 :::110                      :::*                        LISTEN      17706/dovecot
tcp        0      0 :::143                      :::*                        LISTEN      17706/dovecot
...
tcp        0      0 :::25                       :::*                        LISTEN      15865/master
```

**Sobre Windows Server:**

- **Planear:** El objetivo es brindar el servicio Correo Institucional a través de IPv6 sobre el servidor Correo de la Universidad del Cauca, el cual cuenta con un sistema operativo Windows Server 2008 Service Pack 2, bajo el software Exchange 2007, el cual utiliza el servicio IIS, para acceder al correo a través de la WEB a demás del Directorio Activo y DNS, para la relación de los usuarios y dominio IPv6.

**Tabla 3.5.5 Información técnica del servidor Correo, bajo Windows Server 2008**

| | |
|---|---|
| **Nombre** | Server |
| **Sistema Operativo** | Windows Server 2008 Service Pack 2 |
| **Exchange** | 2007 Service Pack 2 |
| **Servicios adicionales** | IIS 7.0<br>Directorio Activo<br>DNS |
| **IPv4** | 10.200.1.38 |

De acuerdo a la información anterior, no es necesario realizar actualizaciones sobre el Sistema Operativo, ni para los Software IIS 7.0 y Exchange 2007, ya que como se indica en la tabla 3.5.6, se cumple con las condiciones.

**Tabla 3.5.6 Validación del soporte IPv6 sobre el servidor Correo, bajo Windows Server 2008**

| | Versión requerida | Versión utilizada | Validación |
|---|---|---|---|
| **Sistema Operativo** | Para Windows Server 2008, IPv6 se encuentra activado de manera predeterminada. Teredo se encuentra habilitado por defecto, pero permanece inactivo hasta que una aplicación o servicio intenta usarlo [25] | Windows Server 2008 | Cumple |
| **IIS** | Soporta IPv6 desde la versión 6.0 [26] | 7.0 | Cumple |
| **Exchange** | 2007 Service Pack 1 [30] | 2007 Service Pack 2 | Cumple |

De acuerdo al plan de direccionamiento planteado, en la sección 2.2.2, se define que la dirección IPv6 a configurar sobre la interfaz del servidor FTP será 2001:13f8:8050:f100::f1e7:5 y owa.unicauca.edu.co será el registro AAAA, que se creará sobre el DNS. Esta información se resume en la tabla 3.5.7.

**Tabla 3.5.7 Configuraciones IPv6, previas, para el servidor Correo, bajo Windows Server 2008**

| Servicio | Sistema Operativo | IPv6 | Registro |
|---|---|---|---|
| IIS | Windows Server 2008 | 2001:13f8:8050:f100::f1e7:5 | owa.unicauca.edu.co |
| Exchange | | | |

- **Hacer:** Se adecuó un contenedor con las especificaciones mencionadas en la tabla 3.5.6, en el cual se configuró la dirección IPv6, se instaló: el servicio de IIS, con soporte WEB, el Directorio Activo y DNS, se vinculó el servidor al dominio creado sobre este, se crearon los registros AAAA, se crearon los usuarios del Directorio Activo, se instaló Exchange y a través de su consola administrativa se crearon los buzones de correo, relacionándolos con los usuarios existentes y se activaron los servicios de entrada (STMP) y salida (POP3 e IMAP4), para permitir conexiones a través del protocolo IPv6.

**Tabla 3.5.8 Pasos realizados para la configuración del servicio Correo con soporte IPv6, bajo Windows Server 2008**

| Paso | Acción |
|---|---|
| 1 | Adecuación del contenedor (Sistema Operativo y Red) |
| 2 | Instalación de IIS 7.0 |
| 3 | Instalación del Directorio Activo y DNS |
| 4 | Vinculación del servidor al dominio creado |
| 5 | Crear usuarios del Directorio Activo |
| 6 | Instalación de Exchange 2007 Service Pack 2 |
| 7 | Creación de buzones y relación con los usuarios existentes. |
| 8 | Configuración de los servicios de entrada y salida para escuchar conexiones a través de IPv6. |

- **Verificar:** Para comprobar que está escuchando por IPv6 el servidor en el puerto 25,110 y 143 se puede utilizar el comando ***netstat –a –n –p tcpv6***

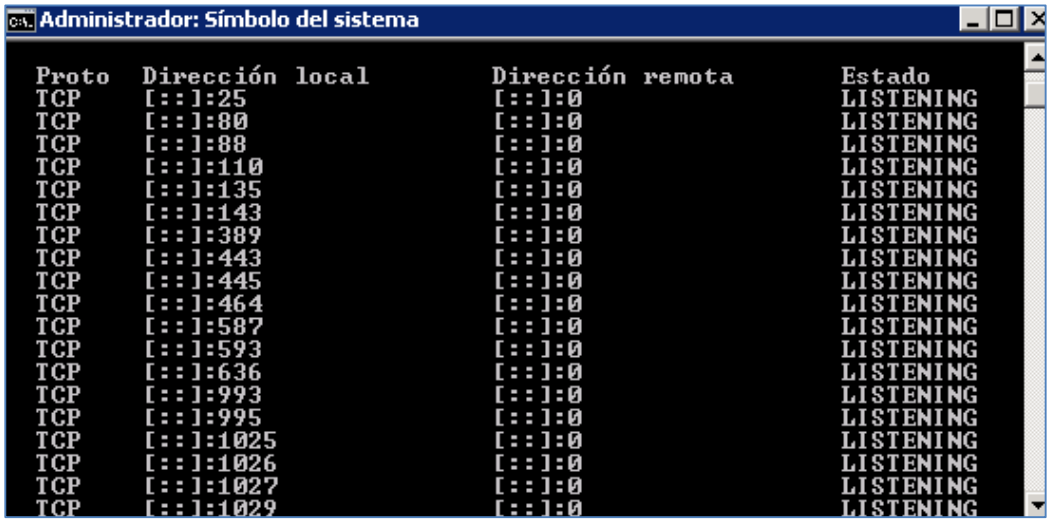
  Se realizan validaciones de envío y recepción de correo desde clientes con IPv6 revisando que en la cabecera del mensaje aparezcan relacionada la dirección IPv6 del servidor indicando que la conexión se estableció a través del nuevo protocolo.

- **Actuar:** Finalmente, para facilitar el acceso a los usuarios, se configura el registro AAAA sobre el DNS interno, dentro del dominio IPv6 y de esta forma acceder al servicio, a través de owa.unicauca.edu.co.

  Como medida de seguridad, se crean políticas en el cortafuegos, en el que solo se permiten acceso a la IP 2001:13f8:8050:f100::f1e7:5, a través del puerto 25, 110 y 143 para permitir el envió y recepción de correos, como también al puerto 80, para permitir el acceso, a través de la WEB.

En la figura 3.5.3, se evidencia los puertos 25, 110, 143 y 80, escuchando a través de IPv6, como también el acceso al Correo, mediante la WEB.

**Figura 3.5.3 Verificación del servicio Correo sobre Windows Server**



# 4 CONCLUSIONES, APORTES Y TRABAJOS FUTUROS

## **4.1** APORTES

La solución propuesta en este trabajo de grado dejó los siguientes aportes

- Metodología de transición *dual-stack* para la red de información de la Universidad del Cauca.
- Solución *dual-stack* en la infraestructura de la red de información de la Universidad del Cauca estableciendo conectividad a la WAN.
- Servicios Internet IPv6 Institucionales operando sobre la red de información de la Universidad del Cauca.

## **4.2** CONCLUSIONES

- La estrategia de migración *dual-stack* representa el método idóneo para la migración a IPv6 debido a que evita incurrir en aspectos técnicos como adquisición y dirección de nuevos equipos, cableado, espacio y herramientas de gestión, por el contrario permite extender la usabilidad de la infraestructura. Sin embargo el no tener un punto de partida desde el cual se pueda desplegar discretamente el protocolo sin incurrir en posibles molestias a los usuarios es engorroso ya que mantener los dos protocolos sobre la misma red si incide en una mayor atención por parte del área encargada en etapas de diseño, implementación y administración.
- La utilización de la metodología Top-Down para la implementación del protocolo IPv6 sobre la red de información de la Universidad del Cauca permitió segmentar los objetivos en subprocesos, posibilitando la visualización de los componentes básico que conforman la red y de esta manera definir adecuadamente los alcances y limitaciones del proyecto.
- La implementación del protocolo IPv6 sobre los servicios Internet de la Universidad del Cauca mediante la metodología PDCA o Ciclo Deaming, permitió definir de manera clara el objetivo, procesos y toma de acciones necesarias para afrontar las dificultades encontradas en el proceso.
- El diseño de IPv6 posee limitaciones físicas que le impiden obtener un rendimiento superior a IPv4. Sin embargo, el diseño del nuevo protocolo incluye características que mejoran el desempeño en otros aspectos. Por ejemplo, la estructura jerárquica de direccionamiento y la eliminación del uso del protocolo NAT, pueden afectar positivamente el desempeño de equipos ubicados en el “backbone” de Internet.

## **4.3** TRABAJOS FUTUROS

A continuación se presentan algunos trabajos que se pueden desarrollar y aportar nuevas funcionalidades a la propuesta mostrada.

- En el ámbito de la seguridad, IPv6 tuvo uno de sus pilares, el protocolo de nueva generación a diferencia de IPv4 define en sus recomendaciones unas cabeceras dedicadas solo a este aspecto lo cual hace que este sea un campo muy amplio por explorar. Dado que la Universidad ya cuenta con la Red y los Servicios Internet IPv6 es conveniente el despliegue de la seguridad sobre esta.

- La Universidad cuenta con una infraestructura de red LAN moderna que ha soportado sin mayores inconvenientes la implantación del protocolo IPv6 en ella. Dado el despliegue de los servicios y la navegación disponible, se propone integrar un sistema de gestión de redes unificado IPv4/IPv6 que complemente la labor administrativa.

- La movilidad en IPv6 también ha sido tenida en cuenta, esto se define en unas recomendaciones específicas y su despliegue necesitaría ante todo la disponibilidad de la red inalámbrica y un proyecto dedicado a esto. Este despliegue es viable a futuro para completar una robusta red IPv6.

- Dado que el actual acceso a la WAN mediante IPv6 se da solo a las redes académicas, se propone plantear una solución que permita tener acceso a Servicios Internet Ipv6 comerciales así como brindar los propios a esta red.

- Con actual auge de los dispositivos móviles y la gran cantidad de aplicaciones que corren sobre la red, adicional a la gran cantidad de direcciones que se requiere asignar, se recomienda definir un esquema mediante el cual se exhorte a la comunidad académica a conocer y explorar esta red, de modo que el nuevo protocolo sea aprovechado.

## BIBLIOGRAFÍA


(1998). *Patente nº RFC 1234.*

[1]U. o. S. C. Sciences Institute, "Internet Protoloco I," in Especificacion del Protocolo vol. RFC 791, ed. California: Marina del Rey, 1981.

[2] J. D. Pascual, "IPv6, Más que un protocolo," Novática, vol. 174, p. 3, Marzo 2005 2005.

[3] E. Majó, "Nueva era en Internet: Se terminó el stock central de direcciones IPv4 de Internet," LACNIC, Montevideo3 de Febrero 2011.

[4] RFC2460 - Deering S. (Cisco), Hinden R. (Nokia). Internet Protocol, Version 6 (IPv6) Especificación. Diciembre 1998.

[5] E. delaParra,"Guia practica para lograr calidad en el servicio." Ediciones Fiscales ISEF, 1997

[6] Microsoft Suport," How to move a DHCP database from a computer that is running Windows Server 2003 to Windows Server 2008" Disponible en: http://support.microsoft.com/kb/962355

[7] Anexo H, entrevista a Martínez Jaime, Universidad del Cauca "Infraestructura Red de Datos", 2011

[8] Anexo H, entrevista a Martínez Jaime. Datos esporádicos recopilados verbalmente.

[9] P. Oppenheimer. Ciscopress.com, "Top-Down Network Design" third edition, p. 7

[10] P. Oppenheimer. Ciscopress.com, "Top-Down Network Design" third edition, p. 15

[11] P. Oppenheimer. Ciscopress.com, "Top-Down Network Design" third edition, p. 25

[12] P. Oppenheimer. Ciscopress.com, "Top-Down Network Design" third edition, p. 59

[13] P. Oppenheimer. Ciscopress.com, "Top-Down Network Design" third edition, p. 60

[14] P. Oppenheimer. Ciscopress.com, "Top-Down Network Design" third edition, p. 120-121

[15] P. Oppenheimer. Ciscopress.com, "Top-Down Network Design" third edition, p. 169

[16] P. Oppenheimer. Ciscopress.com, “Top-Down Network Design” third edition, p. 233
[17] U. d. Cauca. *Filosofía | Universidad del Cauca (Universidad del Cauca ed.)*. Disponible: http:// http://portal.unicauca.edu.co/versionP/acerca-de-unicauca/dependencias/division-de-sistemas/filosofia. [Consultado: Octubre, 2012].

[18] RFC 6177, abstract, disponible en: http://www.rfc-editor.org/rfc/rfc6177.txt

[19] RFC 5375, p. 8, disponible en: http://www.rfc-editor.org/rfc/rfc6177.txt

[20] P. Oppenheimer. Ciscopress.com, “Top-Down Network Design” third edition, p. 83

[21] P. Oppenheimer. Ciscopress.com, “Top-Down Network Design” third edition, p. 22

[22] P. Oppenheimer. Ciscopress.com, “Top-Down Network Design” third edition, p. 101

[23] CISCO IOS IPv6 Feature Mapping, disponible en: http://docwiki.cisco.com/wiki/Cisco_IOS_IPv6_Feature_Mapping

[24] Instalación de IPv6 en plataforma Linux, Mayo 2004, disponible en: http://www.6sos.org/documentos/6SOS_Instalacion_IPv6_Linux_v4_0.pdf

[25] Soporte de IPv6 en sistemas operativos, Santiago, Chile, disponible en: http://www.ipv6.cl/pequena-oficina/soporte-ipv6-en-sistemas-operativos

[26] Despliegue de IPv6, practica de servidores, Santa Cruz, Bolivia, Octubre 2010, disponible en: http://www.6deploy.org/workshops/20101011_santa_cruz_bolivia/DIA2-2-Consulintel_IPv6_ES_SERVERS_v0_3.pdf, p. 21

[27] What's New for Microsoft and FTP in IIS 7?, by Tim Elhajj and R McMurray, January 15, 2008, disponible en: http://www.iis.net/learn/get-started/whats-new-in-iis-7/what39s-new-for-microsoft-and-ftp-in-iis-7

[28] Postfix IPv6 Support, by Dean Strik, disponible en: http://www.postfix.org/IPV6_README.html

[29] Dovecot Configuration File, 2011, disponible en: http://wiki.dovecot.org/MainConfig

[30] IPv6 Support in Exchange 2007 SP1 and SP2, by Microsoft Windows Support, 2011, disponible en: http://technet.microsoft.com/en-us/library/bb629624%28v=exchg.80%29.aspx