

CONFIGURACIÓN DE UNA RED DE NUEVA GENERACIÓN PARA CONECTIVIDAD CON INTERNET RESPALDADO POR UN SERVICIO DNS CON SOPORTE PARA IPv4 E IPv6.

NEW-GENERATION NETWORK CONFIGURATION FOR INTERNET CONNECTIVITY SUPPORTED BY AN IPV4-IPV6-ENABLED DNS SERVICE

Abstract

This article presents the most representative implementation characteristics of an IPv6 island when tested at the High Performance Computing Center at Universidad Distrital (CECAD). Connection and performance tests were made to analyze the internal traffic of the different University subnets. Subsequent testing involved the use of the center's Internet connection through the NAT-PT protocol by means of a recursive-domain-names server as the basis for connectivity and support over native IPv4 and IPv6 structures.

Keywords: DNS, IPv6, IPv4, NAT-PT.

Resumen

Se presentan las características más representativas de la implementación de la isla IPv6 del centro de computación de alto desempeño CECAD, realizando pruebas de conexión y desempeño en el tráfico interno con las subredes de la Universidad Distrital y posteriormente con su conexión a Internet a través del protocolo NAT-PT secundado por un servidor de nombres de dominio recursivo como base de conectividad y soporte sobre estructuras IPv4 e IPv6 nativas.

Palabras clave: DNS, IPv6, IPv4, NAT-PT.

Carlos. A. Martínez

Ingeniero Electrónico, MSc. en Ciencias de la Información y las Comunicaciones, Docente de la Fundación Universitaria Los Libertadores.
carlosm563@hotmail.com

Diego. A. Beltrán

Ingeniero Electrónico, Universidad Distrital "Francisco José de Caldas".
damayab@correo.udistrital.edu.co

Cesar A. Perdomo

Ingeniero Electrónico, MSc. en Teleinformática, de la Universidad Distrital "Francisco José de Caldas, docente de planta de la Facultad de Ingenierías.
cesar.perdomo@gmail.com

Tipo: Artículo de revisión

Fecha de Recepción: Marzo 16 de 2010

Fecha de Aceptación: Mayo 14 de 2010

1. INTRODUCCIÓN

El pasado jueves 3 de febrero del presente año la corporación de internet para la asignación de nombres y números ICANN, anunció en una rueda de prensa la asignación de los últimos dos grandes bloques de direcciones IPv4 a APNIC, la asociación encargada del registro regional de Internet en la zona de Asia y el Pacífico.

En este orden de ideas se prevé que las direcciones IPv4 que ya están asignadas a los diversos organismos regionales que las administran se agoten definitivamente en el mes de Septiembre, es decir que quien necesite una nueva conexión a Internet recibirá una de tipo IPv6.

El nuevo protocolo IPv6, del que ya hace años se dice soluciona todas las carencias del IPv4, reparte direcciones hexadecimales de 128 bits, ocho bloques de cuatro dígitos hexadecimales. Esto permite disponer de un número tan elevado de direcciones únicas que, por lo menos teóricamente, cada dispositivo conectado a la red podría disponer de su propia dirección única y permanente. Actualmente, en la mayoría de los casos, los usuarios finales se conectan a Internet a través de su proveedor de servicios (ISP) con direcciones IPv4 temporales que son reasignadas a otros usuarios a medida que quienes las están utilizando se desconectan de la Red [1].

Como puede advertirse, el posicionamiento de IPv6 y la desaparición de IPv4 no será un proceso de unos pocos años [2], por el contrario estas dos versiones del protocolo de internet deberán coexistir por un periodo de tiempo significativo. Para ello, la IETF ha creado el NGTrans Working Group [4]. Actualmente los esfuerzos de este grupo se han migrado hacia el grupo v6ops (IPv6 Operations group [5]) quienes tiene actualmente encargado las definiciones del proceso de migración.

2. MECANISMOS DE TRANSICIÓN IPV6 IPV4

Existen varios mecanismos de migración IPv6/IPv4, estos mecanismos de traducción se dividen en tres grupos: Dual stack, de traducción y túneles.

El Dual Stack o doble pila, trabaja manteniendo en un mismo dispositivo tanto el stack de IPv4 como el de IPv6, de acuerdo a esto, dependiendo del protocolo que tenga implementado el nodo con el que se pretenda comunicar es la pila Pv4 o IPv6 la que se utilizará.

Los mecanismos de traducción trabajan de manera similar a como lo hace NAT en IPv4, en donde es modificada la cabecera IPv4 a una cabecera IPv6. Dentro de este tipo de mecanismos se encuentran NAT-PT y NAT-64.

Los mecanismo de túneles son muy utilizados cuando se piensa en conectar dos islas IPv6 a través de toda una red IPv4, cuando un paquete IPv6 tiene que atravesar una red que solo es IPv4, el túnel encapsula un paquete IPv6 dentro de un paquete IPv4 para que el mismo pueda viajar a través de estas redes. El paquete es des encapsulado a llegar al nodo IPv6 destino.

3. METODOLOGÍA E IMPLEMENTACIÓN

Dentro del centro de computación de alto desempeño CECAD, se pretende estar a la vanguardia a nivel tecnológico e investigativo, es por esto que se hace necesario empezar a trabajar sobre las redes de nueva generación, encontrando las ventajas e inconvenientes que ellas puedan presentar.

Uno de los objetivos planteados dentro del centro de investigación, es la implementación de una red nativa IPng o IPv6 en la cual se puedan realizar pruebas de conectividad y rendimiento. Para la implementación de esta red es fundamental generar escenarios reales que permitan predecir el comporta-

miento de la misma. Por tal motivo se implemento una topología física formada por Host (con sistema operativo Windows y Linux), un switch capa 2 Catalyst 2960 y un enrutador Cisco 2821.

La IETF ha desarrollado algunos mecanismos para realizar esta transición y asegurar la coexistencia IPv6-IPv4, estos mecanismos implican la utilización de herramientas de ingeniería necesarias para definir estrategias de evolución.

Para el propósito de este trabajo se hizo uso del mecanismo de traducción NAT-PT, el cual se basa en NAT y utiliza las reglas de SIIT para traducir el paquete, aunque presenta algunas diferencias respecto a cómo se traducen las direcciones. Las reglas del algoritmo SIIT para traducir cabeceras IPV4 a IPv6 y viceversa se muestran en la tabla 1.

Tabla 1. Reglas de SIIT para traducción de cabeceras [3].

Campo de la cabecera IPv6	IPv4 →	IPv6	Campo de la cabecera IPv4	IPv6 →	IPv4
Version	4	6	Version	6	4
Traffic Class (Class of Service)	Xxxxxx xx	XXXXXXXX (el TOS y el bit de preferencia se copian)	IP Header Length	N/A	5 (sin opciones)
Flow Label	N/A	0	TOS y precedence	XXXXXXXX	XXXXXX x
Payload Length	X	X+tamaño(cabecera IPv4)+tamaño(opciones IPv4)	Total Length	X	X+ tamaño(cabecera IPv4)
Next Header	X	X	Identification	N/A	0
Hop Limit	X	X+1	Flags	N/A	MF=0 DF=1
Source Address	A.B.C. D	::FFFF:A.B.C.D	Fragment Offset	N/A	0
Destination Address	E.F.G.H	::FFFF:0:E.F.G.H	TTL	X	X+1
			Protocol	Next Header=X	X
			Header Checksum	*	(generado)
			Source Address	::FFFF:A.B.C.D	A.B.C.D
			Destination Address	::FFFF:0:E.F.G.H	E.F.G.H

Mientras SIIT requiere de algún mecanismo complejo de asignación y encaminamiento temporal de direcciones IPv4 a nodos IPv6, en NAT-PT se puede hacer una

asignación de direcciones disponibles (de un conjunto dado) más sencilla. Puede proporcionar comunicación bidireccional entre nodos IPv4 y nodos IPv6 siendo transparente para éstos, además.

Este mecanismo de transición fue escogido por los propósitos claros en los que se basa este proyecto, hacer uso de un servicio DNS que brinde soporte interno a la red de nueva generación y realizar la conexión a Internet, a través del mecanismo NAT-PT.

Dentro del enrutador Cisco 2821 se configuraron los comandos necesarios para el soporte del mecanismo de traducción de NAT-PT con "mapeo" de direcciones. Para que este proceso se realizara correctamente, se habilitó esta traducción en cada interfaz involucrada. Además de esto, la red IPng es vista desde IPv4 por la interfaz pública WAN del enrutador creando una lista de acceso en IPv6 que es asignada a una interfaz gigabit Ethernet configurada en IPv4.

De la misma manera se creo una lista de acceso que por medio del prefijo 2001::/96 traduce cualquier entrada IPv4 para ser vista por la isla IPv6. En adición a esto se configuró la dirección del servidor DNS por medio de NAT-PT estático para asegurar su comunicación con la isla IPv6 (ver Fig. 1).



Fig. 1. Configuración final NAT-PT en el enrutador.

Los nodos de la isla IPv6 nativa, fueron configurados dentro del rango de la dirección asignada a la interfaz LAN del enrutador, específicamente se configuraron las IP 2002:db8:c8::3 y 2001:db8:c8::5 las cuales

fueron escogidas aleatoriamente siguiendo los parámetros direccionamiento IPv6 unicast globales.

El servicio DNS se implementó sobre una red IPv4, pues el objetivo de este servidor no es solo brindar resolución de nombres de dominio a la red IPng, sino también a las otras subredes sobre el protocolo IPv4 del centro de computación de alto desempeño CECAD.

El software utilizado para la creación del servidor DNS fue BIND, el cual proporciona por defecto parámetros robustos de funcionamiento.

Dentro de los parámetros más representativos configurados en el servidor DNS está el que determinados equipos tuvieran permiso para realizar solicitudes, por tal motivo se agregaron las redes o IPs que tendrían acceso, además se asignó la red a la que pertenece el DNS que se identificó con la dirección 10.20.230.0/24, y la dirección pública que esta asignada al enrutador CECAD 200.69.103.22

Tal servidor DNS solo cuenta con zonas maestras locales que pertenecen a nombres dentro del centro. Para conectar estos nodos a Internet y ya que el DNS por sí solo, no es capaz de resolver consultas que no existen dentro de sus zonas, se configuran dos servidores adicionales DNS para reenvío de consultas, que son catalina.udistrital.edu.co (200.69.103.51) y ares.udistrital.edu.co (200.69.103.49), que son los servidores DNS que posee la universidad.

Después de haber elaborado la configuración general del DNS se elaboró la creación de las zonas que componen el CECAD. Las dos zonas que se crearon fueron: cecad.co e ipv6cecad.co incluyendo sus respectivas zonas reversas. La configuración de las zonas incluye parámetros SOA que son identificadores obligatorios del servidor de nombres.

Después de la configuración de los parámetros SOA, se crearon las tablas de resolución de nombres de cada equipo con su respectiva dirección IP, como es una dirección IPv4 se utilizan la asignación tipo A (IPv4). La asignación de "Nombre-IP" se realizó en las zonas cecad.co e ipv6cecad.co, mientras que la asignación "IP-Nombre" se realizó en los reversos respectivamente.

Para la interconexión de la isla IPv6 al DNS y a la red de la universidad UDNET, se propuso el diagrama de red que se observa en la Fig. 2.

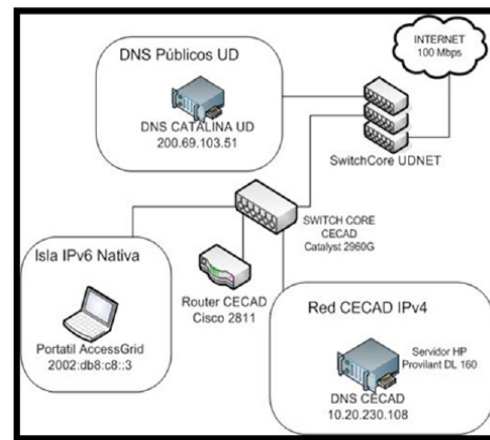


Fig. 2. Esquema conexión IPv6-DNS CECAD.

Este diagrama comprende un nodo en IPv6, el DNS local de CECAD y el DNS público de UDNET. Las consultas del nodo IPV6, primero van dirigidas al DNS CECAD, este a su vez está en la capacidad de redirigir las consultas a los servidores DNS de UDNET o resolverlas por sí mismo a través de consultas anteriormente hechas guardadas en caché.

Cabe destacar que el NAT-PT es el encargado de transformar las consultas de IPv6 a IPv4 y viceversa, es decir, cuando un nodo IPv6 hace una solicitud, esta tiene un formato AAAA, el NAT-PT se encarga de transformar esta consulta en formato A, el DNS a su vez responde en la consulta con una dirección IPv4 pero cuando llega al enruta-

por NAT-PT, este la transforma a IPv6 utilizando el prefijo 2001::/96

4. REALIZACIÓN DE PRUEBAS Y RENDIMIENTO

En este tópico se probó tanto el funcionamiento como el rendimiento en las redes IPv4 e IPv6.

4.1 Pruebas de funcionamiento

Se Incluyeron experimentos en tres diferentes escenarios: a nivel del tráfico interno en el CECAD, a nivel de conexión con las subredes de la Universidad Distrital y finalmente sobre la resolución y conexión de la red de nueva generación a Internet.

En el primer caso, se muestra la conectividad con el servicio DNS (ubicado en el CECAD), de allí puede asumirse que la conectividad interna de la red IPng funciona correctamente pues se visualiza el paso por la puerta de enlace predeterminada para esta subred. La traducción de la dirección del DNS es realizada por el enrutador NAT-PT de manera estática. En la Fig. 3 se muestra la traza de la conexión.

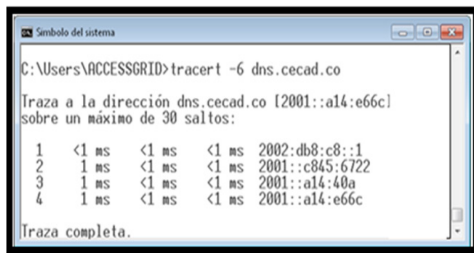


Fig. 3. Traza del nodo IPv6 hacia el DNS IPv4.

En el segundo escenario, ya se hace uso del servicio DNS recursivo (ubicado en una subred externa al centro de alto rendimiento) dentro de la Universidad, allí se puede observar la resolución de direcciones por parte de dicho servicio, que al estar ubicado sobre una red IPv4 necesita de una traducción de petición generada por el NAT-PT (Fig. 4).

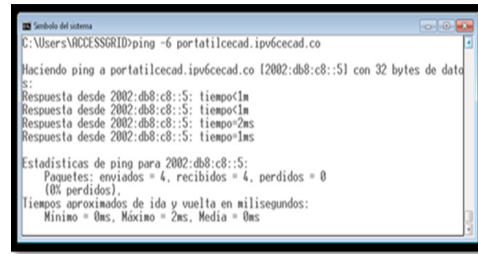


Fig. 4. Conectividad entre nodos IPv6 a través del DNS IPv4.

El tercer escenario en el que se analiza el tráfico de la red IPng, es sobre la conexión de un nodo en esta red con Internet, donde se puede observar la funcionalidad del servicio DNS sobre este escenario, ya que realiza un reenvío de la petición hacia un DNS. Puntualmente en la Fig. 5 se detalla la conectividad por medio del comando de administración PING hacia un sitio web determinado, donde se muestra el tiempo de respuesta y también la dirección IPv4 del sitio embebido sobre el direccionamiento IPv6 realizado por el enrutador NAT-PT.

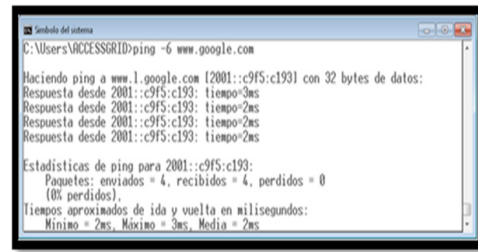


Fig. 5. Conectividad isla IPv6 a Internet.

En la Fig. 6 se captura la traza que realiza la conexión entre el nodo de IPv6 con un sitio web determinado en IPv4. Al igual que en la anterior figura se muestra la dirección IPv4 embebida.

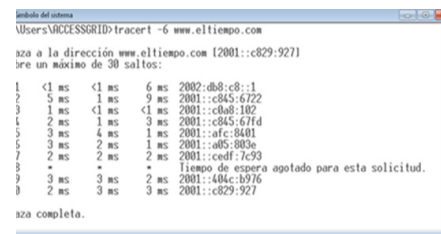


Fig. 6. Traza de un nodo IPv6 a un sitio Web.

A continuación, la Fig. 7, se evidencia la tabla de la traducción NAT-PT realizada en el enrutador usado para este propósito.



Fig. 7. Traducción NAT-PT.

No obstante, dentro de la implementación de la red de nueva generación y su conectividad, se presentó un inconveniente que es preciso mencionarlo para futuras implementaciones. Se trata del uso de los mensajes de actualización; estos mensajes hacen que la memoria del enrutador colapse haciendo que el mismo presente una caída en sus funciones de ruteo y traducción.

Para solucionar este problema fue suficiente con deshabilitar dichos envíos y recepciones automáticos con el uso del comando "undebug all" en la línea de comandos del enrutador. En la Fig. 8 se detalla este suceso, mientras un nodo IPv6 accedía a un sitio web con altos niveles de información.

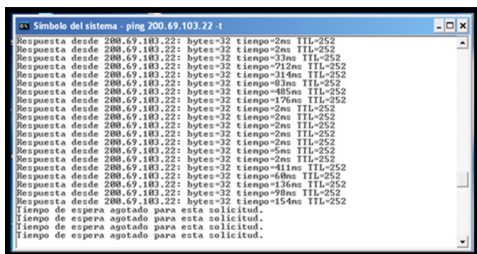


Fig. 8. Colapso del enrutador por los mensajes instantáneos, "debug".

4.2 Pruebas de rendimiento

El software usado para evaluar el rendimiento fue "Iperf", instalado en cada dispositivo utilizado para este propósito.

Se usaron equipos con sistemas operati-

vos Linux (Scientific Linux), Windows Xp y Windows 7. Estos host cuentan con características de red similares: las tarjetas de red son de 1 Gbps al igual que las interfaces del enrutador y del switch utilizados. Además se aseguró que el medio fuese cable FTP categoría 6a para garantizar una alta tasa de transferencia.

El resultado de ancho de banda de transmisión obtenida en las pruebas sobre una red IPv4 se observan en la tabla 2. Cabe aclarar que para cada par, se obtuvo el promedio de un total de 10 muestras.

Tabla 2. Comparación de BW sistemas operativos.

S.O Transmisor	S.O Receptor	Ancho de Banda Mbps
Win 7	Win 7	250
Win 7	Linux	268
Win 7	XP	136
XP	XP	287
XP	Linux	338
XP	Win 7	159
Linux	Linux	938
Linux	Win 7	304
Linux	XP	553

De esta se puede evidenciar que la pareja transmisor-receptor con mejor desempeño sobre la red es en la que los dos sistemas operativos son Linux, teniendo un ancho de banda BW del 93% sobre el valor ideal. En casi el resto de pares, se puede observar que hay una pérdida de ancho de banda de más de un 70 %.

A continuación se realizaron una serie de muestras de una conexión entre dos nodos IPv6 sobre Linux y dos nodos sobre Windows 7. La tabla 3 muestra el desempeño de cada par sobre la red de nueva generación.

Tabla 3. Ancho de banda en la red nativa IPng.

S.O Transmisor	S.O Receptor	Ancho de Banda Mbps
Win 7	Win 7	200
Linux	Linux	930

Como era de esperarse, al igual que el rendimiento sobre la red IPv4 el ancho de banda

en la red IPv6 tuvo mejor desempeño sobre los equipos con sistema operativo Linux.

Además Se llevaron a cabo tres pruebas fundamentales sobre el enrutador: conexión de la isla IPv6 con una red externa IPv4, conexión entre dos subredes dentro del enrutador y por ultimo entre una red IPv4 interna y una IPv4 externa.

En la tabla 4 se puede encontrar el comportamiento del ancho de banda en cada instancia. Cabe aclarar que los equipos usados para estas pruebas fueron el par de equipos Linux, debido a que presentaron un mejor rendimiento en las pruebas anteriores.

Tabla 4. Conexión a través del enrutador Cisco 2821.

Trasmisor	Receptor	ancho de banda Mbps
Nodo IPv6	IPv4 externo	40
Nodo IPv6	IPv4 Interno	662
IPv4 interno	IPv4 Interno	653
IPv4 interno	IPv4 externo	338

Finalmente se realiza una prueba donde se interconectan dos subredes IPv4 de la red UDNET pero no a través de un Router, si no a través de un switch core capa 3.

Al evaluar el ancho de banda en el switch capa 3 3750 se encontraron resultados de 930 Mbps, por lo que se recomienda usar este equipo dentro del centro de computación de alto desempeño CECAD como núcleo de conectividad, ya que su rendimiento obtiene mejores resultados que un enrutador 2821.

5. CONCLUSIONES

La implementación de la red de prueba bajo el protocolo IPv6, posibilita establecer conexiones a otras redes bajo el protocolo IPv4, a través del mecanismo de traducción NAT-PT, complementado con las funciones

del DNS, simplificando la estructura de red y permitiendo la implementación de Servicios Avanzados de Red, fundamentales en ámbitos de investigación, IPv6 Multicasting, e-learning, Voz IP y Computación distribuida (GRID).

La utilización de Software libre, como sistema base para la prestación de servicios de DNS, permite, aprovechar la capacidad de equipos de cómputo, disminución de costos notables con respecto a sistemas comerciales, niveles altos de confiabilidad, versatilidad y eficiencia.

La activación de la función “debug” dentro del enrutador genera una sobrecarga de procesamiento en el dispositivo que impide que funciones como internet IPv4 sobre la red local IPv6 funcionen correctamente poniendo en riesgo la operación normal de la red. Se recomienda que la función debug se utilice solo para pruebas y que en producción se deshabilite.

Tras realizar una revisión teórica de los componentes necesarios para un servidor DNS se encontró que BIND es un buen software para la implementación de este servicio, debido a su actualización constante, soporte, licencia GPL, y abundante documentación.

Según las pruebas realizadas, el rendimiento de una red se puede ver afectado por cada equipo que esté involucrado en la transferencia de paquetes, sus características, su sistema operativo, el tipo de conexión que se realice, entre otros.

En las pruebas realizadas en las redes, se encontró que el mecanismo de traducción NAT-PT consume recursos que se ven reflejados en el ancho de banda por lo que se recomienda la utilización de otros mecanismos de traducción como NAT-64

Referencias Bibliográficas

- [1] Imatica, fin direcciones IPv4, [en línea]. Consultado en Marzo 5 de 2010, disponible en: <http://www.imatica.org/blogs/2011/02/020281562011.html>.
- [2] ABC tecnología, las direcciones Ip se agotan, [en línea]. Consultado en Febrero 14 de 2010, Disponible en <http://www.abc.es/20110202/tecnologia/rww-abci-direcciones-internet-agotan-01102021723.html>
- [3] A. Cabellos. Visión general del protocolo IPv6, [en línea]. Consultado en Enero de 2010, disponible en http://personals.ac.upc.edu/acabello/Albert_Cabellos/Albert_Cabellos/Publications_files/Vision_General_del_protocolo_IPv6-Novatica2005.pdf
- [4] IETF. NGTrans Working Group, [en línea]. Consultado en Marzo 10 de 2010, disponible en <https://www.tools.ietf.org/pdf/draft-ietf-ngtrans-isatap-03.pdf>
- [5] Cisco. The IETF IPv6 Operations Group and The development of a Framework for Deployment of IPv6 into IPv4 Networks, [en línea]. Consultado en Febrero 5 de 2010, Disponible en: http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-2/ipv6_operations_group.html
- [6] G. Tsistsis, P. Srisuresh, Network Address Translation-Protocol Translation (NAT.PT). RFC 2766.
- [7] CCIE. IPv6 NAT-PT Transition, [en línea]. Consultado en Diciembre de 2010, disponible en: <http://cciethebeginning.wordpress.com/2009/07/27/ipv6-nat-pt-transition/>.
- [8] Cisco, Configuration Guide IPv6, [en línea]. Consultado en Marzo 5 de 2010, http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6addrg_bsc_con.html.
- [9] CISCO, IPv6 Integrational and transition, [en línea]. Consultado en Enero 21 de 2010, disponible en http://www.ipv6tf.com.pt/documentos/geral/cisco/ipv6_IntegrationAndTransition_Abr2003.pdf.
- [10] A. MARTÍNEZ, C. DIMATÉ. Diseño de un prototipo de conexión de la red de tecnología avanzada RITA-UD. con la red metropolitana RUMBO bajo IPv6 mediante software libre y el modelo TMN de la UIT-T. 40 h. Trabajo de grado (Ingeniero) Universidad Distrital. Facultad de Ingeniería, Bogotá 2009