ANÁLISIS COMPARATIVO ENTRE IPv6 E IPv4 ENFOCADOS EN LAS ESTRATEGIAS DE SEGURIDAD Y FUNDAMENTADOS EN LA IMPLEMENTACIÓN SOBRE UN ESCENARIO REAL

CARLOS ALBERTO GONZÁLEZ PEÑALOZA
JUAN RICARDO TURBAY RAMÍREZ

UNIVERSIDAD AUTONOMA DE BUCARAMANGA
FACULTAD DE INGENIERIA DE SISTEMAS
TELECOMUNICACIONES Y TECNOLOGIAS WEB
BUCARAMANGA
2008

ANÁLISIS COMPARATIVO ENTRE IPv6 E IPv4 ENFOCADOS EN LAS ESTRATEGIAS DE SEGURIDAD Y FUNDAMENTADOS EN LA IMPLEMENTACIÓN SOBRE UN ESCENARIO REAL

CARLOS ALBERTO GONZÁLEZ PEÑALOZA

JUAN RICARDO TURBAY RAMÍREZ

Trabajo de grado para optar al título de

Ingeniero de Sistemas

Director

Ing. Carlos Gilberto Delgado Beltrán

UNIVERSIDAD AUTONOMA DE BUCARAMANGA

FACULTAD DE INGENIERIA DE SISTEMAS

TELECOMUNICACIONES Y TECNOLOGIAS WEB

BUCARAMANGA

2008

Nota de Aceptación

_____

_____

_____

_____

Firma del Jurado

_____

Firma del Jurado

_____

Firma del Director

Bucaramanga, 4 Febrero de 2008

TABLA DE CONTENIDO

pág.

INTRODUCCIÓN 18

1. MODELO OSI 20

1.1 ARQUITECTUTA TCP/IP (Transmission Control Protocol – Protocolo de Control de Transmisión / Internet Protocol – Protocolo de Internet) 22

1.2 PROTOCOLO IPv4 23

1.2.1 Unicast 24

1.2.2 Multicast 26

1.2.3 Broadcast 26

1.3 LIMITACIONDES DE IPV4 27

1.4 PROTOCOLO IPV 27

1.5 DIFERENCIAS ENTRE IPv4 E IPv6 29

2. ESTRATEGIAS DE IMPLANTACIÓN 31

2.1 DOBLE PILA DE PROTOCOLOS (DOUBLE STACK IP) 32

2.1.1 Configuración de direcciones 32

2.1.2 Autoconfiguración de direcciones sin estado 33

2.1.3 Autoconfiguración de direcciones con estado 33

2.2 TUNELES 33

2.2.1 Túnel configurado 35

2.2.2 Túnel automático 36

2.2.3 Túnel 6 to 4 37

2.2.4 Túnel 6 over 4 37

2.3 TRADUCCIÓN DE ENCABEZADO Y DE PROTOCOLO 38

2.3.1 SIIT (Stateless IP/ICMP Traslation Algorithm) 38

2.3.2 NAT-PT 39

2.4 PROTOCOLO DE SEGURIDAD IP (IPsec RFC 2401) 40

2.4.1 Encabezado de autenticación (AH) RFC 4302 41

2.4.2 ESP (Encapsulating Security Payload) RFC 4303 42

2.4.3 IPsec en modo transporte 43

2.4.4 IPsec en modo túnel 43

3. ESCENARIOS PROPUESTOS 44

3.1 ESCENARIO 1 RED SOLO IPv4 45

3.1.1 Descripción del escenario 45

3.1.2 Configuración Router 1 46

3.1.3 Configuración Router 2 46

3.1.4 Configuración Router 3 46

3.2 ESCENARIO 2 ISLA IPv6 CONECTADAS ENTRE SI USANDO TUNELES 47

3.2.1 Descripción del escenario 47

3.2.2 Configuración del Router 1 48

3.2.3 Configuración del Router 2 49

3.2.4 Configuración del Router 3 50

3.3 ESCENARIO 3 DUAL SNACK 51

3.3.1 Descripción del escenario 51

3.3.2 Configuración del Router 1 52

3.3.3 Configuración del Router 2 52

3.3.4 Configuración del Router 3 53

3.4 ESCENARIO 4 RED SOLO IPv6 54

3.4.1 Descripción del escenario 54

3.4.2 Configuración del Router 1 55

3.4.3 Configuración del Router 2 55

3.4.4 Configuración del Router 3 56

4. PRUEBAS DE SEGURIDAD 57

4.1 PRUEBA 1 57

4.1.1 Resultados de la prueba 1 58

4.2 PRUEBA 2 62

4.2.1 Activación del IPsec AH e IPsec ESP sobre Windows XPSP2 62

4.2.2 Resultados de la prueba 2 72

4.3 PRUEBA 3 77

4.3.1 Pasos de la Compilación E Instalación Del Servidor Apache En Fedora Core 6 77

4.3.2 Configuración del servidor Apache 79

4.3.3 Resultados de la prueba 3 81

4.4 PRUEBA 4 84

4.4.1 Activación del IPsec sobre Linux Fedora Core 6 85

4.4.2 Resultados de la prueba 2 92

5. SÍNTESIS DE RESULTADOS 96

6. CONCLUSIONES 99

7. TRABAJOS FUTUROS 102

BIBLIOGRAFÍA 103

LISTA DE TABLAS

pág.

Tabla 1. Diferencias entre IPv4 e IPv6 29

Tabla 2. Tabla comparativa de resultados. 96

LISTA DE FIGURAS

pág.

Figura 1. Modelo de referencia OSI. 21

Figura 2. Muestra las capas del modelo TCP/IP. 23

Figura 3. Muestra la estructura de una dirección de clase A. 25

Figura 4. Muestra la estructura de una dirección de clase B. 25

Figura 5. Muestra la estructura de una dirección de clase C. 26

Figura 6. Esquema básico de un túnel. 34

Figura 7. Encapsulado y desencapsulado de un paquete IPv6. 35

Figura 8. Túnel configurado. 35

Figura 9. Representa un túnel automático. 36

Figura 10. Representa un túnel 6 to 4. 37

Figura 11. Representa un túnel 6 over 4. 38

Figura 12. Paquete protegido con AH. 42

Figura 13. Paquete protegido con ESP. 42

Figura 14. Red solo IPv4. 45

Figura 15. Islas IPv6 contactadas mediante túneles. 47

Figura 16. Escenario Dual Stack. 51

Figura 17. Escenario Red solo IPv6. 54

Figura 18. Resultados de la prueba 1 para el escenario 1. 58

Figura 19. Resultados de la prueba 1 para el escenario 2. 59

Figura 20. Resultados de la prueba 1 para el escenario 3. 60

Figura 21. Resultados de la prueba 1 para el escenario 4. 61

Figura 22. Ventana Local Security Settings. 63

Figura 23. Asistente para la creación de una política de seguridad. 63

Figura 24. Métodos de autenticación para la política de seguridad. 64

Figura 25. Ventana para la creación de reglas de seguridad. 65

Figura 26. Tunnel End Point. 66

Figura 27. Tipos de red. 66

Figura 28. Métodos de autenticación, para la regla de seguridad. 67

Figura 29. Filtros de tráfico. 68

Figura 30. Acción del Filtro de tráfico. 68

Figura 31. Métodos de seguridad. Fuente. 69

Figura 32. Selección del tipo de encabezado IPSec. 70

Figura 33. Edición de una política de seguridad. 71

Figura 34. Métodos de seguridad y selección de encabezado IPSec. 72

Figura 35. Resultados de la prueba 2, sobre el escenario 1, utilizando IPSec AH. 73

Figura 36. Resultados de la prueba 2, sobre el escenario 1, utilizando IPSec ESP. 73

Figura 37. Resultados de la prueba 2, sobre el escenario 2, utilizando IPSec AH. 74

Figura 38. Resultados de la prueba 2, sobre el escenario 2, utilizando IPSec ESP. 74

Figura 39. Resultados de la prueba 2, sobre el escenario 3, utilizando IPSec AH. 75

Figura 40. Resultados de la prueba 2, sobre el escenario 3, utilizando Con IPSec ESP habilitado. 75

Figura 41. Resultados de la prueba 2, sobre el escenario 4, utilizando IPSec AH. 76

Figura 42. Resultados de la prueba 2, sobre el escenario 4, utilizando IPSec ESP. 76

Figura 43. Ventana de servicios de Linux Fedora Core 6. 80

Figura 44. Resultados de la prueba 3, sobre el escenario 1. 81

Figura 45. Resultados de la prueba 3, sobre el escenario 2. 82

Figura 46. Resultados de la prueba 3, sobre el escenario 3, usando IPv4. 83

Figura 47. Resultados de la prueba 3, sobre el escenario 3, usando IPv6. 83

Figura 48. Resultados de la prueba 3, sobre el escenario 4. 84

Figura 49. Ventana de configuración de red. 86

Figura 50. Asistente para la configuración de IPSec. 87

Figura 51. Sobrenombre para la conexión IPSec. 88

Figura 52. Tipo de conexión. 89

Figura 53. Modo de encriptación. 90

Figura 54. Red remota. 90

Figura 55. Creación de llaves. 91

Figura 56. Resultados de la prueba 4, sobre el escenario 1. 92

Figura 57. Resultados de la prueba 4, sobre el escenario 2. 93

Figura 58. Resultados de la prueba 4, sobre el escenario 3. 94

Figura 59. Resultados de la prueba 4, sobre el escenario 4. 95

RESUMEN

Debido a los constantes avances en el área de las telecomunicaciones como los servicios de telefonía celular, el wimax, palms o agendas electrónicas, entre otros, el nivel de exigencia, con respecto a la seguridad de los datos, la confiabilidad y las transferencias de información es mayor. Adicionalmente, existe una creciente escasez de direcciones IP, debido al incremento de personas con acceso a Internet, lo cual ha suscitado el desarrollo de IPv6 como protocolo que remplazará el estándar actual IPv4. La presente investigación intenta elaborar una metodología para la migración, valorando primordialmente los aspectos relacionados con la exigencia en la configuración, las limitaciones en costos, tanto en software como en hardware y el nivel de seguridad. De esta manera se usarán dos estrategias para la implementación de IPv6: los Túneles Configurados y Dual Stack, evaluando cual es la estrategia más eficiente para la migración e igualmente observando cual es el sistema operativo sobre el cual es más efectivo realizar la implementación.

Palabras claves: protocolos de Internet, interconexión de sistemas, métodos de migración, criptografía, seguridad de redes.

INTRODUCCIÓN

Debido a los constantes avances en el área de las telecomunicaciones como: los servicios de telefonía celular, el wimax, palms o agendas electrónicas, entre otros, el nivel de exigencia, con respecto a la seguridad de los datos, la confiabilidad y las transferencias de información es mayor. Adicionalmente, existe una creciente escasez de direcciones IP, debido al incremento de personas con acceso a Internet, lo cual ha suscitado el desarrollo de IPv6 como protocolo que remplazará el estándar actual IPv4.

Para el desarrollo de este proyecto se enfatizará en la medición y posterior documentación del nivel de exigencia en configuración, limitaciones en costos, tanto en hardware como software y el nivel de seguridad de cuatro escenarios que representan la migración de IPv4 a IPv6. Para lograr este objetivo se usaran herramientas como analizadores de tráfico y sniffers

Los escenarios a desarrollar, teniendo en cuenta un orden secuencial en el proceso de migración serán:

- Una red sólo IPv4 que representa el estado actual de la mayor parte de las redes mundiales.

- Redes IPv6 (islas) conectadas usando túneles sobre la infraestructura IP actual, es la segunda etapa en la migración de IPv4 a IPv6.

- Una red que permite la utilización tanto de IPv4 como de IPv6 (Dual Stack).

- Una red sólo IPv6, que representa el punto final de la migración.

1. MODELO OSI

En principio, el desarrollo de las redes LAN (Local Area Network – Red de Area Local) y WAN (Wide Area Network – Red de Area Amplia) se hacía de manera desordenada.

En la década de los 80, nuevos desarrollos produjeron un aumento en la cantidad de redes y en su tamaño, debido a que las empresas notaron los beneficios que la tecnología de redes traía consigo, tales como: el ahorro de dinero y el crecimiento de la productividad. Pero, surgió también un grave problema de incompatibilidad.

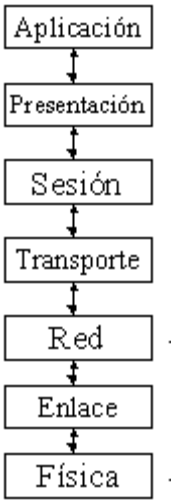
Para combatir éste problema la ISO (International Organization for Standardization – Organización Internacional para la Normalización) estudió algunos modelos existentes de la época como DECNET, SNA (Systems Network Architecture – Arquitectura de Redes de Sistemas) y TCP\IP. El objetivo del estudio, era encontrar un conjunto de reglas aplicables, de forma general, a todas las redes y desarrollar su propio modelo. Este fue bautizado como "OSI "(Open Systems Interconnection Reference Model – Modelo de referencia para la Interconexión de Sistemas Abiertos). Los reglamentos de la ISO, no sólo han tenido gran influencia en la parte técnica sino, también en ingenieros, manufactureros, la economía y en la sociedad a nivel mundial. Esta organización ha incrementado los niveles de calidad, seguridad, eficiencia y la calidad de intercambio.

El modelo OSI fue lanzado en 1984 y, hasta el día de hoy, proporciona a los fabricantes un conjunto de estándares que aseguran una mayor compatibilidad e

interoperabilidad entre los distintos tipos de tecnología de red utilizada por las empresas a escala mundial.[1]

El modelo de referencia OSI, está compuesto por siete capas, cada una con una función especifica. Las capas se muestran en la figura 1.

Figura 1. Modelo de referencia OSI.



Fuente. Modelo OSI. Cisco Certified Network Associated, Second edition, Todd Lammle, SYBEX. Copyright 2000 Sybex Inc. p. 5.

- Capa de aplicación: se encarga de proporcionar los servicios al usuario.

- Capa de presentación: se encarga de convertir e interpretar los datos que se utilizarán en el nivel de aplicación.

[1] SANTANA Darwin. All rights reserved. IPv6: Nueva Generación Protocolo de Internet. [En línea]. Santo Domingo. 2006. [Citada el 18 de agosto del 2007]. Disponible en Internet en: <http://www.lac.ipv6tf.org/docs/tutoriales/IPv6-LACTF.pdf>.

- Capa de sesión: se encarga de los aspectos de la comunicación. Por ejemplo, el control de los tiempos.

- Capa de transporte: se encarga de transportar la información, de una manera confiable, hasta el destino.

- Capa de red: se encarga de enviar los datos hacia el destino, eligiendo la ruta más confiable.

- Capa de enlace: se encarga del control de flujo de datos, la sincronización y los posibles errores que se produzcan.

- Capa física: se encarga de los aspectos físicos de la conexión, tales como el hardware y el medio de transmisión.

1.1 ARQUITECTURA TCP/IP (Transmission Control Protocol – Protocolo de Control de Transmisión / Internet Protocol – Protocolo de Internet)

Aunque el modelo OSI, es el modelo de referencia para las nuevas tecnologías de red, es debido al gran éxito de la Internet que TCP\IP es el modelo más utilizado en la actualidad. El modelo TCP\IP es una colección de protocolos estándares de la industria, diseñados para la interconexión de redes. El TCP y el IP fueron desarrollados por el Departamento de Defensa de los Estados Unidos para conectar un número de diferentes redes (diseñadas por distintos distribuidores) a una red de redes, o sea la Internet. Cubre unas necesidades básicas que todo usuario necesita, algunas de éstas son: la transferencia de archivos, el correo electrónico, el “log in” automático y otras. Todo esto se hace con un inmenso número de clientes y de sistemas de servidores.

Figura 2. Muestra las capas del modelo TCP/IP.

Fuente. PARKER Timothy, Ph.D, Capas del modelo TCP/IP. TCP/IP Unleashed, SAMS publishing. Copyright 1996 by Sams publishings. p. 27.

- Capa de aplicación: se encarga de la autenticación y terminación de servicios.
- Capa de Transporte: se encarga de los flujos, tanto de entrada, como de salida
- Capa de Red: tiene como función proveer el enrutamiento a los paquetes.
- Capa Física: hace referencia al cableado o conexión física.

1.2 PROTOCOLO IPv4

El IPv4 es la cuarta iteración del protocolo Internet y es la primera versión del protocolo en ser, mundialmente desplegado. Si ignoramos a su sucesor, IPv6,

seria considerado como el único protocolo usado en la Internet. Es un protocolo orientado al uso de información y es un servicio de red, que no provee características específicas en la recuperación de información pérdida o corrupta. El IPv4 no garantiza el envío.

Este protocolo usa direcciones de 32 bits (4- byte), lo cual limita el espacio. Esta razón ha estimulado el desarrollo y la implementación del IPv6, que aún se encuentra en una etapa temprana.

El principal propósito, de esté protocolo, es la interconexión de sistemas para la comunicación y envió de paquetes llamados datagramas, que van desde un emisor a un destino, bajo la red. Las direcciones IP son únicas y universales. Eso quiere decir que no pueden haber direcciones repetidas y que la única manera para poder conectarnos a la Internet es usando una dirección IP. Cada dispositivo tiene su propia IP que lo identifica dentro de la red, además están expresadas de manera binaria y conformada por unos y ceros. Debido a que este tipo de dirección es difícil de recordar, se le asignó una notación decimal, donde cada cuatro números decimales de 0 – 255 es separado por un punto. Cada número decimal es conocido como un octeto que representa 8 bits (1 byte).

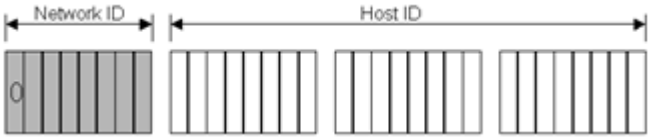
Cabe tener en cuenta, que cada nodo hace parte de una red y a la vez tiene una o más interfaces. Se puede habilitar el protocolo TCP\IP a cada una de ellas, para luego asignarle de manera manual o automática, una dirección IPv4.

Según los estándares de direccionamiento, IPv4 tiene tres tipos de direcciones IPs que son:

1.2.1 Unicast. Es un sistema en donde se envía información desde un único emisor a un único receptor.

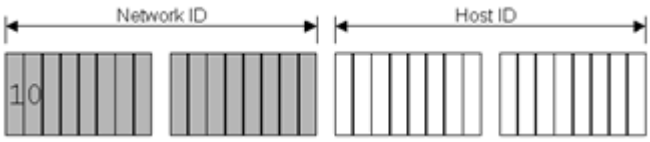
Este tipo de direcciones son las que se encargan de identificar la localidad de la interfase dentro de la red. Un ejemplo sería la dirección del lugar en donde vivimos. Una dirección que puede identificar el sitio en donde estamos o, el bloque donde nos encontramos. Las direcciones unicast son únicas y sólo tienen un tipo de formato. Todas las direcciones tipo IPv4 incluyen un prefijo, que identifica la subred y otra porción para identificar el host. Las clases A, B y C son direcciones de tipo unicast. Las clases de tipo D son para multicast y las E son para uso experimental.

Figura 3. Muestra la estructura de una dirección de clase A.



Fuente. Networking and Access Technologies. Microsoft Corporation. All rights reserved. Estructura de una dirección IPv4 clase A. [En línea]. 2007. [Citado el 13 de julio del 2007]. Disponible en Internet en: < http://technet.microsoft.com/en-us/library/bb726995.aspx >.

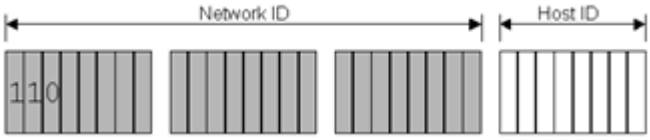
Figura 4. Muestra la estructura de una dirección de clase B.



Fuente., Ibíd.

En la figura anterior, los primeros 16 bits son para uso particular de la red y los últimos 16 bits son para uso del host. Sin embargo, los dos bits de mayor rango, siempre son dados con el número 10, como se ve en la imagen.

Figura 5. Muestra la estructura de una dirección de clase C.



Fuente., Ibíd.

Este tipo de direcciones son asignadas a redes pequeñas. Los primeros 24 bits de una dirección de tipo C, hacen referencia a una red en particular y los últimos 8 bits son para la identificación del host. Los bits más importantes para una clase B son 10. En el caso de una clase C, los bits más importantes son 110.

1.2.2 Multicast: (IPv4). Tienen como objetivo enviar información, simultáneamente, a determinados destinos, se categoriza como clase D donde los bits más importantes son 1110. Estas direcciones son asignadas a una o más redes y su tipo de comunicación es uno a muchos.

Multicast es una tecnología que reduce el tráfico de envío de información, debido a que la envía, simultáneamente, y usa una corriente de transmisión. Es parecido a la radio o la televisión en el sentido que, solamente, aquellos usuarios que estén conectados a sus receptores (escogiendo una frecuencia que les interese) recibirá la información. Cada data grama IP, cuya dirección de destino comience con 1110, es un data grama multicast.

1.2.3 Broadcast. Este sistema de comunicación es empleado para enviar información desde un destino a varios destinos. En este caso sólo hay un emisor, pero la información es enviada a todos los receptores. Estas direcciones son

asignadas a toda clase de redes y son reservadas para uso experimental. El mayor orden de bits en este tipo de direcciones es 1111.

1.3 LIMITACIONES DE IPv4

Algunas de las limitaciones del IPv4 son el crecimiento de las tablas de enrutamiento, calidad de servicio, seguridad y el número de combinaciones posibles de direcciones que es, aproximadamente de 4.294'967.296 IPs. Esta cifra vendría a ser insignificante si la comparamos con el constante crecimiento de la Internet y la exigencia, por parte de las personas por el uso de dispositivos móviles, PDAs, carros con mapa de navegación por vía satelital y otros. Estas nuevas tecnologías, que están surgiendo, y que requieren de una identificación (IP) para acceder a la red (Internet), son la causa principal de la escasez de IPs. En la actualidad, la dirección IPv4 no suministra información acerca de su router. Por esta razón, la intención del IPv6 es la de asignar una subred a cada cliente. De acuerdo a estudios realizados, no se ha encontrado una razón en el que IPv4 tenga ventajas técnicas sobre el IPv6. Hasta el día de hoy se calcula que las dos terceras partes de las direcciones que ofrece IPv4 ya están asignadas.

1.4 PROTOCOLO IPv6

IPv6, fue diseñado por el IETF (Internet Engineering Task Force), organización que se encarga de la estandarización de los protocolos en Internet, es el nuevo protocolo para las comunicaciones. En cuanto al diseño de este nuevo programa, se tuvo en cuenta un aspecto, de suma importancia, que es la necesidad de un mercado futurista. Estos mercados exigirán y se basarán en seguridad, eficiencia y

variabilidad. El protocolo ha sido desarrollado para funcionar con protocolos ya existentes. Se podrá hacer creando túneles para cargar los “paquetes” IPv6, lo que permitirá el fortalecimiento de la actual Internet sin requerir de cambios obstructivos. Los usuarios podrán hacer el cambio progresivamente y de una manera natural y voluntaria.

Uno de los cambios más significativos ha sido el incremento del tamaño de la dirección, pasando de 32 a 128 bits[2]. Este aumento se refleja en una mayor cantidad de direcciones usables.

Teniendo en cuenta lo anterior, la cantidad de direcciones disponibles en IPv6, es una cifra de 39 dígitos.

2^{128-1}: 340282366920938463463374607431768211455 = 39 dígitos

Pero, como se ve, es una cantidad de números bastante difícil de llegar a recordar. Es así, como se buscó darle el mismo esquema que a las direcciones IPv4, pero representadas en forma hexadecimal.

Una vez dada esta forma representativa, las direcciones quedan del siguiente modo:

2^{128-1}: 0xffffffffffffffffffffffffffffffff = 32 dígitos

Si se observa bien, la forma de representación anterior, puede acarrear a que a veces hiciera falta un dígito o que hubiera dígitos de más. Por lo tanto, los mismos diseñadores de IPv6, optaron por separar cada bloque de 16 bits (4 dígitos hexadecimales) con el signo (:), tal como se muestra a continuación:

---

[2] HINDEN, R. Cisco Systems All rights reserved. IP Versión 6 Addressing Architecture. [En línea]. 1998. [Citada el 18 de agosto del 2006.]. Disponible en Internet en: < http://www.ietf.org/rfc/rfc2373.txt>

2^{128-1}: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Para hacer mucho más sencilla la representación anterior de una dirección IPv6, a cada uno de los bloques de 16 dígitos se le omite el primer cero.

Ejemplo:

3ffe:ffff:0100:f101:0210:a4ff:fee3 → Como se puede observar, los ceros que se encuentran en rojo, son los primeros de cada bloque, por lo tanto se omiten.

↓ ↓

3ffe:ffff:100:f101:210:a4ff:fee3

Cuando se tiene una secuencia con varios ceros seguidos, entonces éstos son reemplazados con (::).

Ejemplo:

3ffe:ffff:100:f101:0:0:0:1 -> 3ffe:ffff:100:f101::1

Por lo tanto, la mayor reducción posible es:

0000:0000:0000:0000:0000:0000:0000:0001 -> ::1

1.5 DIFERENCIAS ENTRE IPv4 e IPv6

Tabla 1. Diferencias entre IPv4 e IPv6.

IPv4	IPv6
La longitud es de 32 bits. Parte para la identificación de la red y otra para el host	La longitud es de 128 bits. 64 bits asignados para la red y los otros 64 bits restantes para la host

La compatibilidad con IPSec es opcional.	La compatibilidad con IPSec es obligatoria.
Usa máscara de Red.	No usa máscara de Red
La fragmentación es posible en ambos enrutadores y en el host de envío.	La fragmentación no es posible en los enrutadores. Sólo es posible en el host de envío.
Los tipos de direcciones que usa son Unicast, Multicast y Broadcast.	Los tipos de direcciones que usa son Unicast, Multicast y Anycast.
El tamaño del encabezado varia de 20 – 60 bytes.	El tamaño es de 40 bytes
Las direcciones de difusión se utilizan para enviar tráfico a todos los nodos de una subred.	No hay direcciones de difusión de IPv6. En su lugar, se utiliza una dirección de multidifusión para todos los nodos de ámbito local de vínculo.
El filtrado de paquetes funciona bajo un firewall integrado al protocolo TCP\IP	No soporta
El encabezado incluye opciones.	Todos los datos opcionales se mueven a extensiones de encabezado IPv6.

Fuente. REATEGUI, Ivette. IPv6 Project Status. Diferencias entre IPv4 e IPv6. [En línea]. 2002. [Citado el 14 de abril del 2007]. Disponible en Internet en: <http://rds.yahoo.com/>

2. ESTRATEGIAS DE IMPLANTACIÓN

Actualmente, IPv4 es el protocolo dominante en las redes mundiales. Realizar una migración, completa y a gran escala, de todos los nodos IPv4 existentes a IPv6, conllevaría a unos costos en organización y hardware insostenibles.

Una posible solución a ésta problema es desarrollar métodos que permitan que el IPv4 e IPv6 operen juntos en las redes por el momento sin mayor problema y sin tener que hacer fuertes inversiones de capital. El uso de alguno de estos métodos es necesario, al menos por ahora, debido a que la cantidad de redes IPv6 juntas no alcanzan el 1 %, lo cual dificulta su interconexión. Por lo tanto, se hace necesario usar la infraestructura IPv4.

Existen 3 mecanismos básicos desarrollados para ayudar a la transición de IPv4 a IPv6. Estos son:

- Doble pila de protocolos (Double stack IP).
- Túneles.
- Traducción de encabezado y de protocolo.

2.1 DOBLE PILA DE PROTOCOLOS (DOUBLE STACK IP)

Este método representa la forma más sencilla de comunicar un nodo IPv4 con uno IPv6 y consiste en darle a este último un soporte completo sobre IPv4, de tal forma que el nodo IPv6 con Double Stack IP tenga la capacidad de enviar y recibir paquetes, tanto de IPv6, como de IPv4.[3]

Un nodo con Double Stack IP puede operar en 1 de 3 estados diferentes:

- Con el protocolo IPv4 activado y el IPv6 desactivado: En éste modo, el nodo sólo puede entender de paquetes IPv4.

- Con el protocolo IPv4 desactivado y el IPv6 activado: En éste modo, el nodo sólo puede entender de paquetes IPv6.

- Con ambos protocolos activados: En éste modo, el nodo puede entender tanto paquetes IPv4 como IPv6.

2.1.1 Configuración de Direcciones. Ya que, en éste tipo de estrategia, los nodos entienden ambos protocolos, es necesario configurarle ambos tipos de direcciones; de 32 bits para IPv4 y de 128 bits para IPv6.

Para obtener las direcciones IPv4, un nodo con Double Stack IP, puede usar DCHP (Dinamic Host Configuration Protocol) o sea, el protocolo de configuración dinámica de servidores

[3] NORDMARK. E Sun Microsystems All rights reserved. Basic Transition Mechanisms for IPv6 Hosts and Routers. [En línea]. 2005. [Citada el 11 de agosto del 2006.]. Disponible en Internet en: <http://www.ietf.org/rfc/rfc4213.txt >

Un nodo Double Stack IP puede obtener una dirección IPv6 de varias maneras. La más destacada es el uso del DCHPV6 o auto configuración de direcciones con estado o sin estado.

2.1.2 Autoconfiguración De Direcciones Sin Estado. En éste modo, un nodo puede obtener una dirección IPv6 combinando información local anunciada por los routers. Tiene como ventaja, el hecho de que no requiere configuración alguna de routers ni configuración manual de servidor alguno.

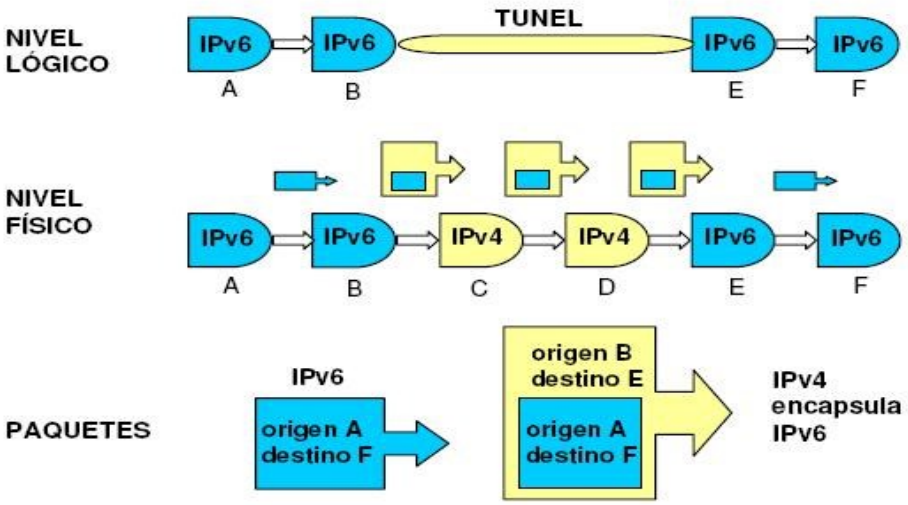
2.1.3 Autoconfiguración De Direcciones Con Estado. La principal desventaja del método Double Stack IP es que, si algún nodo lo utiliza, el resto de nodos también tiene que hacerlo. Esto, en una red grande puede hacer difícil la migración.

2.2 TÚNELES

Los túneles son otra de las estrategias más comunes para la implementación de IPv6, ya que permiten la implantación de IPv6 utilizando la infraestructura IPv4 existente. Este proceso es totalmente transparente para el usuario. Los hay de 2 clases estáticos, y dinámicos.

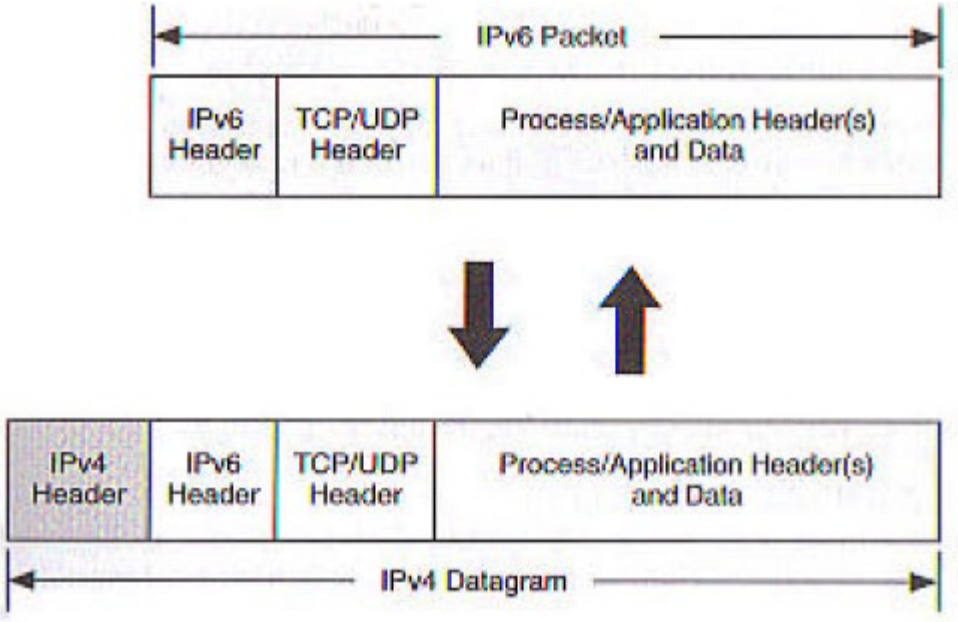
Tal como se puede apreciar en la figura 6, un túnel sirve como puente de comunicación entre 2 nodos IPv6. El túnel está montado sobre una infraestructura IPv4 común. Para que esto sea posible, el paquete IPv6, antes de pasar por el túnel, es convertido (encapsulado) a un paquete IPv4. De ésta manera podrá viajar sin inconvenientes, y antes de llegar al otro lado, podrá transformarse (desencapsulado) a su forma original.

Figura 6. Esquema básico de un túnel.



Fuente. CAMARGO, Edwin. Tesis sobre plan de transición del protocolo de IPv4 a IPv6 en la Universidad Industrial de Santander. [En línea]. Bucaramanga 2006. [Citada 18 de agostos de 2007]. Disponible en Internet en: <http://www.uis.edu.co>

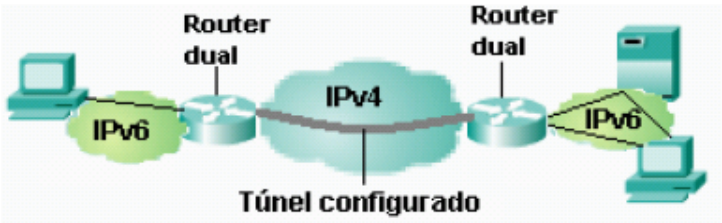
Figura 7. Encapsulado y desencapsulado de un paquete IPv6.



Fuente. How IPv6 Works. Microsoft Corporation. All rights reserved. Encapsulado y desencapsulado de un paquete IPv6. [En línea]. 2006. [Citado el 18 de agosto del 2007]. Disponible en Internet en: <http://technet2.microsoft.com/WindowsServer/en/library>.

2.2.1 Túnel Configurado. Es un tipo de túnel que tiene como función principal, conectar nodos aislados IPv6 utilizando la infraestructura IPv4. La siguiente figura representa un túnel configurado.

Figura 8. Túnel configurado.



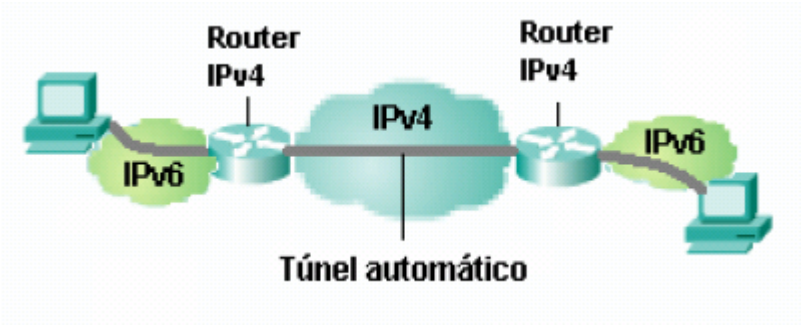
Fuente., Ibíd.

En éste tipo de túnel, los routers duales, que están a los extremos del túnel, tienen direcciones configuradas tanto IPv6 como IPv4. En algún momento, uno hará de encapsulador y el otro de desencapsulador. El enrutamiento, dentro del túnel, se hace mediante las tablas de enrutamiento IPv4. Es decir, utilizando una dirección y una máscara. Este proceso lo hace el router que encapsula.

Por desgracia, este tipo de túneles no son perfectos. Tienen, como gran desventaja, el frenar la escalabilidad de la red, y requieren de una ardua configuración manual por parte del usuario.

2.2.2 Túnel Automático. Su configuración es simple, en este tipo de túnel, la información del router se pasa por el túnel. Por esta razón, puede ser enviada por diferentes redes, al final de cualquiera de los túneles, con una configuración mínima. Permite a nodos, tanto IPv4 y IPv6, comunicarse utilizando una infraestructura IPv4 ya existente. Éste tipo de túnel se usa para (el) host, que se encuentren sin routers IPv6 en el enlace.

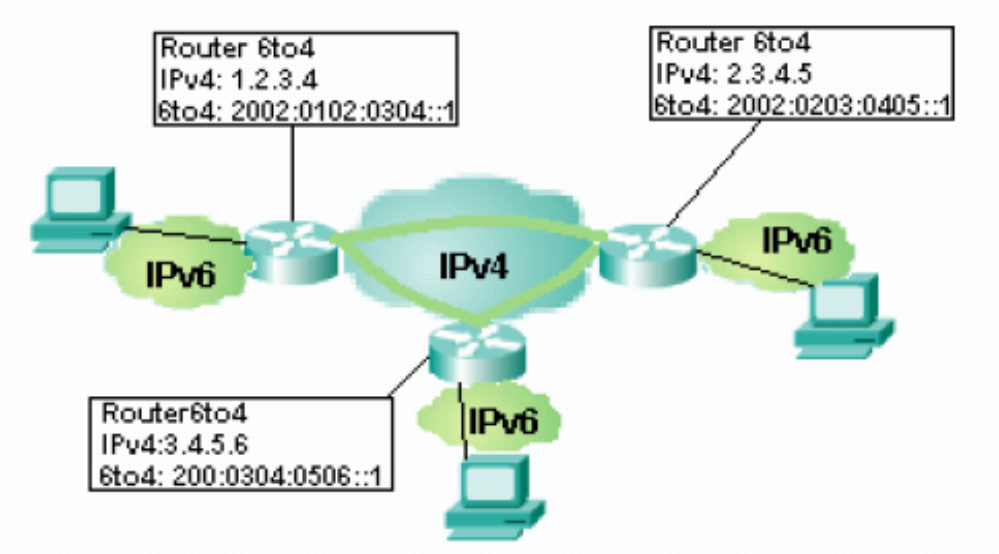
Figura 9. Representa un túnel automático.



Fuente., Ibíd.

2.2.3 Túnel 6 to 4. Es un túnel de tipo dinámico, por lo tanto, no requiere de configuración por parte del usuario y permite la comunicación de nodos IPv6 utilizando redes IPv4. Cada nodo, en este tipo de túnel, se identifica con un prefijo 2002:/16 seguido de la dirección IP del router frontera. La mayor ventaja de este túnel es que los túneles serán creados automáticamente, y así el usuario no queda restringido al enrutamiento del 6bone, que a veces puede ser insuficiente.

Figura 10. Representa un túnel 6 to 4.

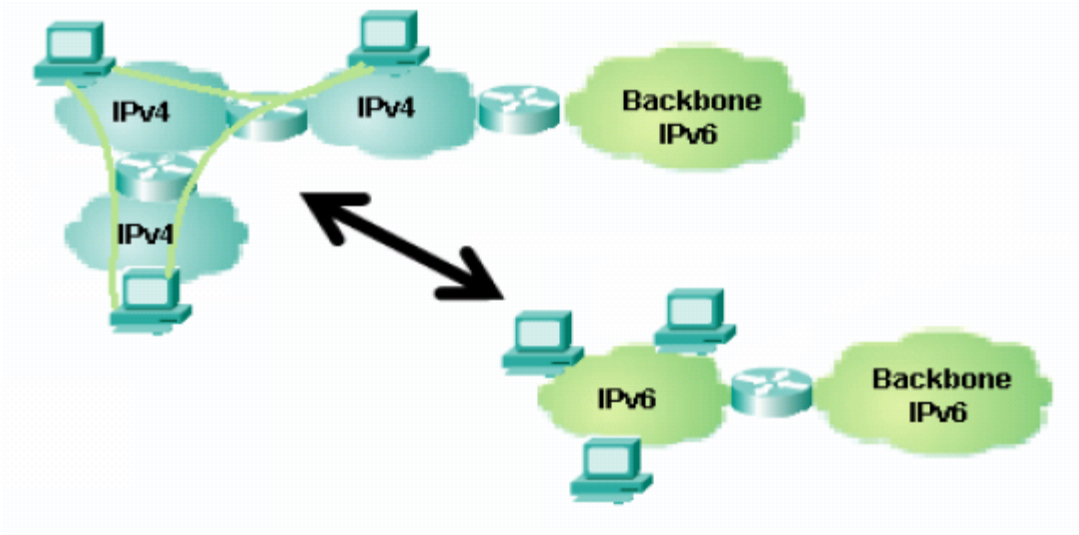


Fuente., Ibíd.

2.2.4 Túnel 6 over 4. Es un túnel, de tipo dinámico, que no requiere de configuración previa. Permite la conexión de nodos IPv6, dispersos en redes IPv4, formando una LAN virtual

Además el proceso de encontrar a los vecinos se hace mediante multicast.

Figura 11. Representa un túnel 6 over 4.



Fuente., Ibíd.

2.3 TRADUCCIÓN DE ENCABEZADO Y DE PROTOCOLO

2.3.1 SIIT (Stateless Ip/Icmp Translation Algorithm). Es el primero de este tipo de métodos. Este algoritmo traduce entre encabezados de IPv6 e IPv4. La traducción se ve limitada a la cabecera IP. Este algoritmo no realiza control de estado, por lo que, la traducción se hace individualmente a cada paquete[4].

Este método se desarrolló con el fin de permitir la comunicación entre PCs que manejan IPv6 o IPv4.

[4] SANTANA, Darwin. All rights reserved. IPv6: Nueva Generación Protocolo de Internet. [En línea]. Santo Domingo 2006. [Citada el 18 de agosto del 2007]. Disponible en Internet en: <http://www.lac.ipv6tf.org/docs/tutoriales/IPv6-LACTF.pdf>.

2.3.2 NAT-PT (Traducción De Direcciones De Red Nat-Pt - Network Address Translation – Protocol Translation). Es mecanismo fue desarrollado para permitir la comunicación transparente entre nodos que entienden sólo IPv6 con nodos que entienden sólo IPv4.

Como su nombre lo indica, este método, está compuesto por NAT (Traducción de direcciones de red) y por PT (Traducción de protocolo).

El NAT, utilizado en este protocolo, es muy similar al NAT IPv4. La diferencia radica en que, el NAT IPv4, traduce un grupo de direcciones IPv4 privadas a una o varias direcciones IPv4 públicas. El NAT utilizado en NAT-PT, traduce un grupo de direcciones IPv6 a una o varias direcciones IPv4 públicas.

Existen 2 variaciones de NAT-PT, en un NAT-PT tradicional, las sesiones son unidireccionales, saliendo de la red IPv6. En la segunda variación, conocida como NAT-PT bidireccional, las sesiones pueden ser iniciadas desde host en una red IPv4, así como, desde una red IPv6.[5]

Debido a la traducción de protocolos y cambio de direcciones, IPSec no tiene efecto alguno, cuando se usa cualquiera de las variaciones de NAT-PT[6].

---

[5] Plan de transición del protocolo de IPV4 a IPv6 en la Universidad Industrial de Santander, [Citada el 18 de agosto del 2006].

[6] BENOIT, Lourdelet. Cisco System All rights reserved. Cisco IOS NAT-PT for IPv6. [En línea]. 2003. [Citada el 18 de agosto del 2006]. Disponible en Internet en: <http://www.cisco.com/application/pdf/en/us/guest/tech/tk361/c1550/ccmigration_09186a008018221e.pdf>.

2.4 PROTOCOLO DE SEGURIDAD IP (IPSec RFC 2401)

Es una estructura de estándares abiertos para asegurar la privacidad y proteger las comunicaciones. Se maneja bajo el protocolo IP, mediante el manejo de servicios de seguridad criptográficos.

Los dos puntos fuertes de IPsec son:

- La protección de los paquetes IP
- La defensa ante posibles ataques a la red

Los dos puntos, mencionados anteriormente, son implementados mediante servicios basados en criptografía, seguridad en los protocolos, manejos de contraseñas adecuados, y otros. También posee la característica de bloquear tráfico no deseado.[7]

Algunas de las propiedades que brinda IPsec para la protección en las comunicaciones son:

Integridad de los datos: ayuda a proteger los datos de posibles modificaciones, no autorizadas, durante el proceso de envío. Se asegura, que la información que recibe el receptor, sea la misma enviada por el emisor. También implementa una técnica de criptografía Hash, basada en la verificación de una suma, quien envía el paquete, tanto como el que lo recibe, deben tener la llave correcta para poder calcular la respectiva suma. De ésta manera, si la suma llega a ser diferente, cuando el paquete es recibido, entonces éste es descartado.

[7] Technet. Microsoft Corporation All rights reserved. Introducing IPSec. [En línea]. 2007. [Citada el 14 de agosto del 2007]. Disponible en Internet en: < http://www.microsoft.com >.

Confidencialidad (encriptación): esta propiedad permite asegurar que los datos puedan ser desencriptados y vistos solo por las personas previstas. Por lo tanto el usuario puede tener la certeza de que si los datos caen en manos ajenas, este no podrá revisar su contenido ni divulgarlo

Autentificación del origen de datos: ayuda a garantizar que la información enviada, provenga de de una sola máquina que contenga la llave clave.

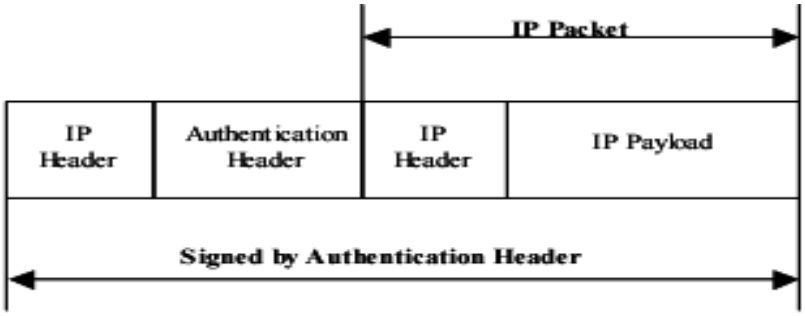
Filtrado de paquetes: esta técnica consiste en la posibilidad de configurar interfaces de modo que sean capaces de aceptar o descartar tráfico basado en diferentes criterios como el protocolo de transmisión de datos (TCP) y los puertos bajo el protocolo de data gramas de usuario (UDP). También identifica la hora de envió.

IPSec funciona agregando su propio encabezado de seguridad a cada paquete que es transmitido. Entre los encabezados con los que cuenta IPSec están AH (Authentication Header RFC 4302) y ESP (Encapsulation Security Payload 4303).

2.4.1 Encabezado de autenticación (AH) RFC 4302. Proporciona integridad sin conexión y autenticidad del origen de datos para data gramas IP y para proporcionar protección contra reenvíos.[8]

[8] KENT, S. BBN Technologies All rights reserved. IP Authentication Header RFC 4302. [En línea]. 2005. [Citada el 16 de agosto del 2006]. Disponible en Internet en: <ftp://ftp.rfc-editor.org/in-notes/rfc4302.txt>.

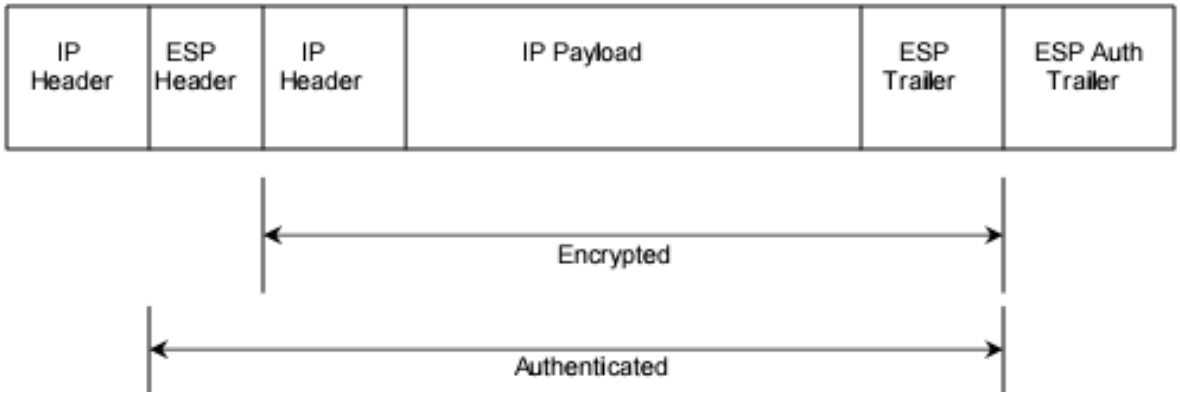
Figura 12. Paquete protegido con AH.



Fuente. OIF OPTICAL INTERNETWORKING FORUM. [En línea]. 2003. [Citada el 18 de Enero de 2007]. Disponible en Internet en :<http://rds.yahoo.com>

2.4.2 ESP (Encapsulating Security Payload) RFC 4303. Tiene como función proveer autenticidad a (de) los datos, integridad, protección de reenvió y confidencialidad de los datos.[9]

Figura 13. Paquete protegido con ESP.



Fuente., Ibíd.

[9] KENT, S. BBN Technologies All rights reserved. IP Authentication Header RFC 4302. [En línea]. 2005. [Citada el 16 de agosto Del 2006]. Disponible en Internet en: < ftp://ftp.rfc-editor.org/in-notes/rfc4303.txt >.

IPSec tiene 2 modos de operación: modo transporte y modo túnel, además sobre cada modo, IPSec permite usar los encabezados AH o ESP, cabe recalcar que el funcionamiento de los encabezados de IPSec es igual en los 2 modos en los que funciona IPSec.

2.4.3 IPSec en modo transporte. Este es el modo en el que trabaja por defecto IPSec, se utiliza en comunicaciones de extremo a extremo (cliente y servidor). En éste modo se provee protección usando ESP o AH solo al IP payload.[10]

2.4.4 IPSec en modo túnel. Estando éste modo en funcionamiento se provee protección tanto al encabezado IP como al IP payload, es decir todo el paquete IP es protegido usando AH o ESP. IPSec en modo túnel es muy útil cuando se requiere proteger tráfico entre diferentes redes, donde este trafico atraviesa zonas no son seguras.[11]

El modo túnel se usa para escenarios como:

- Gateway a gateway
- Servidor a gateway
- Servidor a servidor

[10] Microsoft techNet. Microsoft Corporation. All rights reserved. Transport Mode. [En línea]. 2005. [Citada el 16 de agosto del 2007]. Disponible en Internet en: < http://technet2.microsoft.com/ >.

[11] Microsoft techNet. Microsoft Corporation. All rights reserved. Transport Mode. [En línea]. 2005. [Citada el 11 de agosto del 2007]. Disponible en Internet en: < http://technet2.microsoft.com/windowsserver/en/library/ >.

3. ESCENARIOS PROPUESTOS

Los escenarios de migración de IPv4 a IPv6 propuestos para el desarrollo de este proyecto son cuatro, para su implementación se utilizaron los siguientes elementos:

- Routers cisco 2620xm equipados con el IOS c2600-advipservicesk9-mz.123-18, este IOS fue seleccionado por que brinda soporte en:
  - IPv6 (Internet Protocol Version 6).
  - IPv6 Routing: RIP for IPv6 (RIPng).
  - ICMPv6 (Internet Control Message Protocol for IPv6).
  - Configuración Stateless para IPv6.
  - IPv6 Tunneling.[12]

- Switches Cisco catalyst 2950

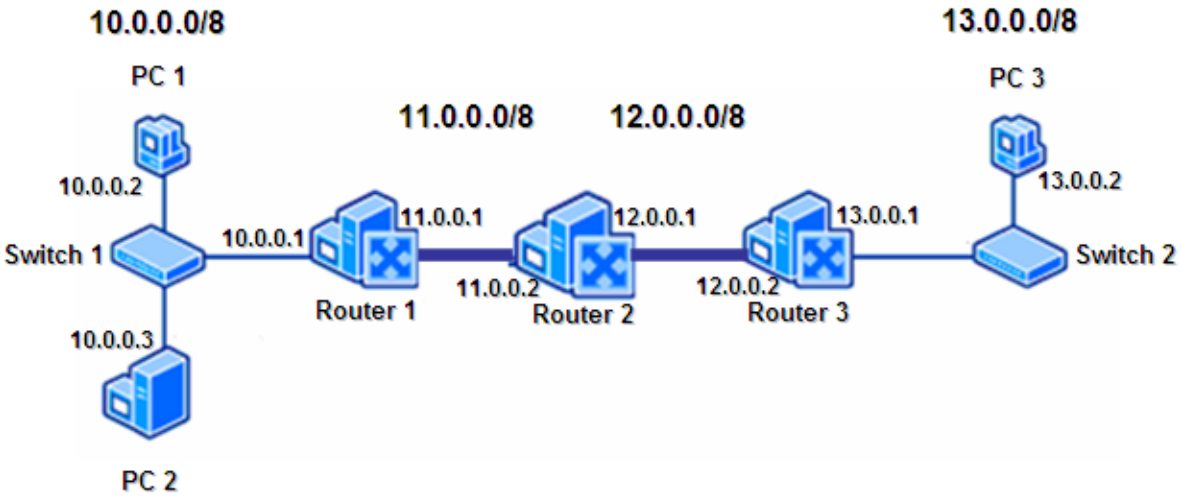
- Hubs Cisco

Las topologías y configuraciones de cada escenario se presentan a continuación:

[12] Cisco System. Cisco System Inc. All rights reserved. Cisco Feature Navigator. [En línea]. 1992. [Citada el 11 de agosto del 2006.]. Disponible en Internet en: < http://www.cisco.com/ >.

3.1 ESCENARIO 1 Red solo IPV4

Figura 14. Red solo IPv4.



Fuente. CISCO, Products Configuration Guide, 2007. [En línea]. [Citado en Marzo 10 del 2007] Disponible en Internet en: <http://www.cisco.com/en/US/products/ >

3.1.1 Descripción del escenario. El primer escenario esta compuesto por tres routers cisco 2620xm, equipados con un IOS (Internetwork Operating System) de la serie Advance IP Services, versión 12.3 (18), además cuenta con dos 2 switches Cisco Catalyst 2950 para la conmutación LAN. El protocolo de enrutamiento configurado es RIP versión 1. Para la interconexión entre routers se utiliza cable serial V35 con conectores WIC (tarjeta de interfaz WAN), para la conexión de router a switch se utiliza cable cruzado UTP categoría 5e y de switch a PC se utiliza cable directo UTP categoría 5e. Sobre este escenario, el router intermedio representa Internet (WAN), además todas las interfaces de los equipos activos tienen configuradas direcciones solo IPv4.

3.1.2 Configuración Router 1

```
interface FastEthernet0/0
        ip address 10.0.0.1 255.0.0.0
        duplex auto
        speed auto

interface Serial0/1
        ip address 11.0.0.1 255.0.0.0

router rip
        network 10.0.0.0
        network 11.0.0.0
```

3.1.3 Configuración Router 2

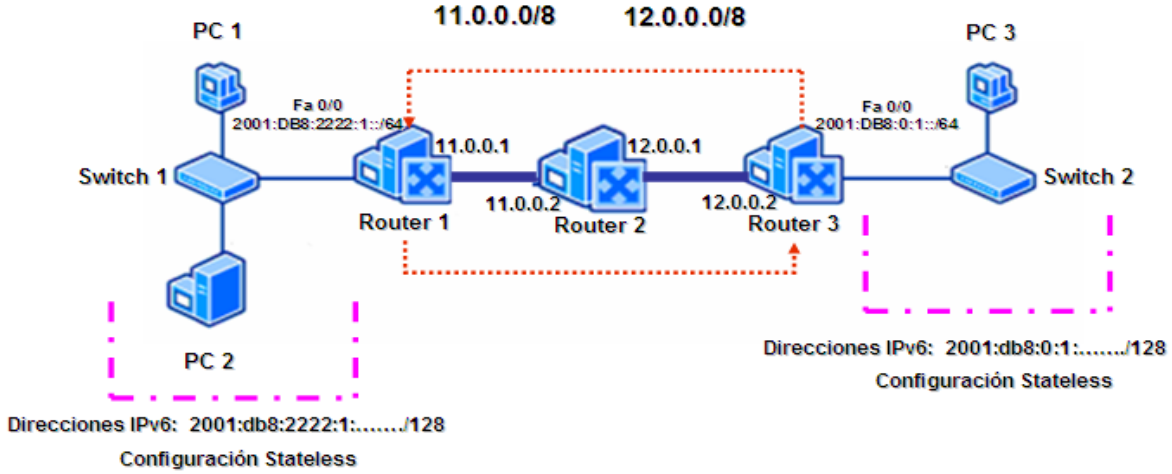
```
interface Serial0/0
        ip address 11.0.0.2 255.0.0.0
        clock rate 56000

interface Serial0/1
        ip address 12.0.0.1 255.0.0.0

router rip
        network 11.0.0.0
        network 12.0.0.0
```

3.1.4 Configuración Router 3

```
interface FastEthernet0/0
        ip address 13.0.0.1 255.0.0.0
        duplex auto
        speed auto

interface Serial0/0
        ip address 12.0.0.2 255.0.0.0
        clock rate 56000

router rip
        network 12.0.0.0
        network 13.0.0.0
```

3.2 ESCENARIO 2 Islas IPV6 conectadas entre si usando Túneles

Figura 15. Islas IPv6 contactadas mediante túneles.



Fuente., Ibíd.

3.2.1 Descripción del escenario. El segundo escenario esta compuesto por tres routers cisco 2620xm, equipados con un IOS de la serie Advance IP Services, versión 12.3 (18), además cuenta con dos 2 switches Cisco Catalyst 2950 para la conmutación LAN. Para la interconexión entre routers se usa cable serial V35 con conectores WIC, para la conexión de router a switch se utiliza cable cruzado UTP categoría 5e y de switch a PC se utiliza cable directo UTP categoría 5e.

Las líneas púrpuras sobre el grafico, representan islas IPv6, es decir, son redes que utilizan un esquema de direccionamiento IPv6, las direcciones asignadas a los host ubicados en cada isla, se realiza a través de configuración Stateless (sobre esta configuración, el mismo prefijo, por ejemplo 2001:db8:2222:1, es asignado a todos los host ubicados en la misma red, el resto de la dirección es generada automáticamente por el host, de acuerdo al número y tipo de interfaz de red que utilice). Las líneas punteadas rojas representan los túneles configurados, hay dos líneas, ya que una representa el flujo de datos de salida y la otra de regreso.

Los routers de los extremos tienen configurados tanto direcciones IPv4 como IPv6, además utilizan enrutamiento RIP versión 1 y RIPng, el router intermedio el cual representa Internet, solo utiliza enrutamiento IPv4.

3.2.2 Configuración Router 1

```
ipv6 unicast-routing

interface Tunnel0
        no ip address
        ipv6 address 3FFE:B00:C18:1::3/127
        ipv6 rip red enable
        tunnel source Serial0/1
```

```
        tunnel destination 12.0.0.2
        tunnel mode ipv6ip

interface FastEthernet0/0
        no ip address
        duplex auto
        speed auto
        ipv6 address 2001:DB8:2222:1::/64
        ipv6 rip red enable

interface Serial0/1
        ip address 11.0.0.1 255.0.0.0

router rip
        network 11.0.0.0

ipv6 route 2001:DB8:0:1::/64 Tunnel0
ipv6 router rip red
```

3.2.3 Configuración Router 2

```
interface Serial0/0
        ip address 11.0.0.2 255.0.0.0
        clock rate 56000

interface Serial0/1
        ip address 12.0.0.1 255.0.0.0

router rip
```

```
        network 11.0.0.0
        network 12.0.0.0
```

3.2.4 Configuración Router 3

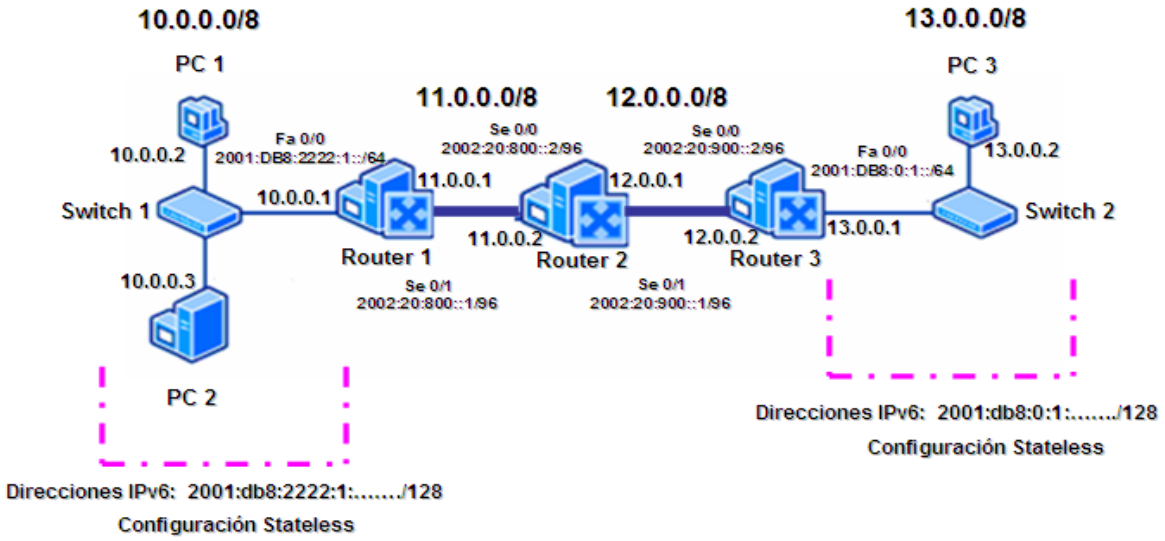
```
ipv6 unicast-routing

interface Tunnel0
        no ip address
        ipv6 address 3FFE:B00:C18:1::2/127
        ipv6 rip red enable
        tunnel source Serial0/0
        tunnel destination 11.0.0.1
        tunnel mode ipv6ip

interface FastEthernet0/0
        no ip address
        duplex auto
        speed auto
        ipv6 address 2001:DB8:0:1::/64
        ipv6 rip red enable

interface Serial0/0
        ip address 12.0.0.2 255.0.0.0
        no fair-queue
        clock rate 56000

router rip
        network 12.0.0.0
```

ipv6 route 2002::/16 Tunnel0

ipv6 router rip red

3.3 ESCENARIO 3 DUAL SNACK

Figura 16. Escenario Dual Stack.



Fuente., Ibíd.

3.3.1 Descripción del escenario. El tercer escenario esta compuesto por tres routers cisco 2620xm, equipados con un IOS de la serie Advance IP Services, versión 12.3 (18), además cuenta con dos 2 switches Cisco Catalyst 2950 para la conmutación LAN. Para la interconexión entre routers se utiliza cable serial V35 con conectores WIC, para la conexión de router a switch se utiliza cable cruzado UTP categoría 5e y de switch a PC se utiliza cable directo UTP categoría 5e.

Las líneas púrpuras sobre el grafico, representan redes duales, es decir, son redes que utilizan al mismo tiempo un esquema de direccionamiento IPv4 e IPv6. Las direcciones IPv6 asignadas a los host ubicados en cada red dual, se realiza a través de configuración Stateless.

Todos los equipos activos tienen configurados tanto direcciones IPv4 como IPv6, para el enrutamiento IPv4 se utiliza RIP versión 1 y para enrutamiento IPv6 se utiliza RIPng.

3.3.2 Configuración Router 1

```
ipv6 unicast-routing

interface FastEthernet0/0
        ip address 10.0.0.1 255.0.0.0
        duplex auto
        speed auto
        ipv6 address 2001:DB8:2222:1::/64
        ipv6 rip red enable

interface Serial0/1
        ip address 11.0.0.1 255.0.0.0
        ipv6 address 2002:20:800::1/96
        ipv6 rip red enable

router rip
        network 10.0.0.0
        network 11.0.0.0
```

3.3.3 Configuración Router 2

```
ipv6 unicast-routing

interface Serial0/0
        ip address 11.0.0.2 255.0.0.0
        ipv6 address 2002:20:800::2/96
        ipv6 rip red enable
        no fair-queue
        clock rate 56000

interface Serial0/1
        ip address 12.0.0.1 255.0.0.0
        ipv6 address 2002:20:900::1/96
        ipv6 rip red enable

router rip
        network 11.0.0.0
        network 12.0.0.0

ipv6 router rip red
```

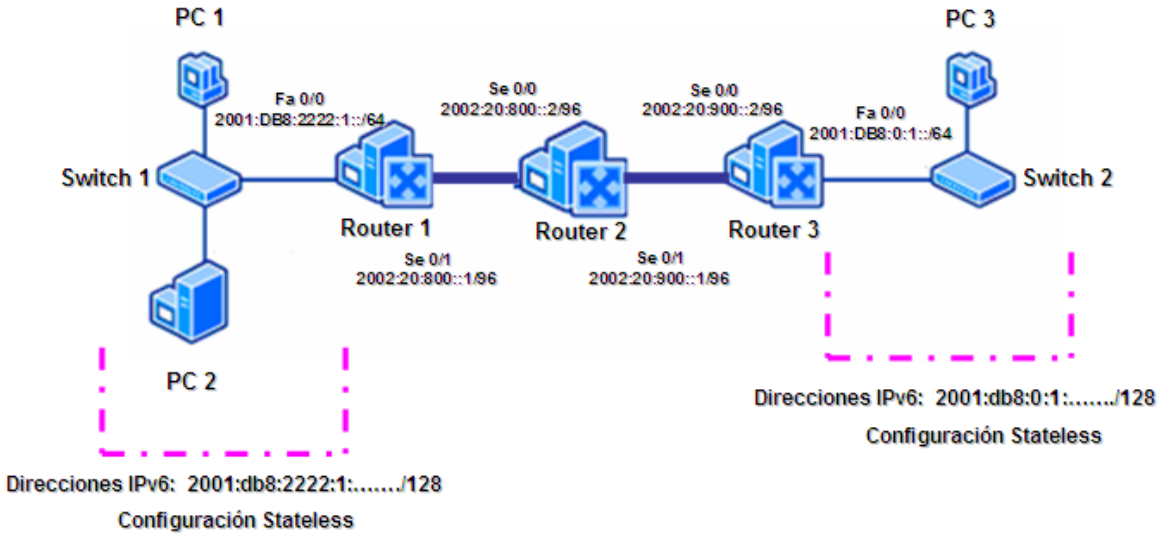
3.3.4 Configuración Router 3

```
ipv6 unicast-routing

interface FastEthernet0/0
        ip address 13.0.0.1 255.0.0.0
        duplex auto
```

```
        speed auto
        ipv6 address 2001:DB8:0:1::/64
        ipv6 rip red enable

interface Serial0/0
        ip address 12.0.0.2 255.0.0.0
        ipv6 address 2002:20:900::2/96
        ipv6 rip red enable
        no fair-queue
        clock rate 56000

router rip
        network 12.0.0.0
        network 13.0.0.0

ipv6 router rip red
```

3.4 ESCENARIO 4 RED SOLO IPV6

Figura 17. Escenario Red solo IPv6.



Fuente., Ibíd.

3.4.1 Descripción del escenario. El cuarto escenario esta compuesto por tres routers cisco 2620xm, equipados con un IOS de la serie Advance IP Services, versión 12.3 (18), además cuenta con dos 2 switches Cisco Catalyst 2950 para la conmutación LAN. El protocolo de enrutamiento configurado es RIPng. Para la interconexión entre routers se utiliza cable serial V35 con conectores WIC, para la conexión de router a switch se utiliza cable cruzado UTP categoría 5e y de switch a PC se utiliza cable directo UTP categoría 5e. Sobre este escenario, el router intermedio representa Internet (WAN), además todas las interfaces de los equipos activos tienen configuradas direcciones solo IPv6.

3.4.2 Configuración Router 1

```
ipv6 unicast-routing

Interface FastEthernet0/0
        no ip address
        duplex auto
        speed auto
        ipv6 address 2001:DB8:2222:1::/64
        ipv6 rip red enable

interface Serial0/1
        no ip address
        ipv6 address 2002:20:800::1/96
        ipv6 rip red enable

ipv6 router rip red
```

3.4.3 Configuración Router 2

```
ipv6 unicast-routing

interface Serial0/0
        no ip address
        ipv6 address 2002:20:800::2/96
        ipv6 rip red enable
        clock rate 56000

interface Serial0/1
```

```
        no ip address
        ipv6 address 2002:20:900::1/96
        ipv6 rip red enable

ipv6 router rip red
```

3.4.4 Configuración Router 3

```
ipv6 unicast-routing

interface FastEthernet0/0
        no ip address
        duplex auto
        speed auto
        ipv6 address 2001:DB8:0:1::/64
        ipv6 rip red enable

interface Serial0/0
        no ip address
        ipv6 address 2002:20:900::2/96
        ipv6 rip red enable
        no fair-queue
        clock rate 56000

ipv6 router rip red
```

4. PRUEBAS DE SEGURIDAD

El plan de pruebas fue diseñado teniendo en cuenta dos parámetros de seguridad, estos serán usados para medir el desempeño de cada protocolo en cada uno de los escenarios propuestos y permitir identificar cual protocolo es más seguro, los parámetros son:

- Autenticación del origen de los datos: permite verificar si los datos son enviados por una maquina autorizada.

- Confidencialidad de los datos: se define como protección en contra la revisión y divulgación no autorizada de información.

Las pruebas de seguridad realizadas sobre cada uno de los escenarios se muestran a continuación, aparte de una breve explicación de la dinámica y objetivos de la prueba, se presentaran los resultados que tuvo cada escenario, en cada prueba implementada.

4.1 PRUEBA 1

Esta prueba consiste básicamente en conectarse a un router utilizando el servicio de Telnet, el router fue configurado para solicitar a los usuarios una clave VTY (esta clave es: cisco) para poder utilizar el servicio. Paralelo al ingreso del password un sniffer (Wireshark anteriormente conocido como ethereal) será plantado en una interfaz Ethernet de un PC, con el propósito de tratar de capturar

la contraseña de Telnet en el momento que sea enviada al router para culminar el proceso de autenticación.

4.1.1 Resultados De La Prueba 1

- Para el escenario 1

Figura 18. Resultados de la prueba 1 para el escenario 1.

```
  1 0.000000   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  2 0.226514   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=1 Win=4096 Len=0
  3 0.226615   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  4 0.454463   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=2 Win=4095 Len=0
  5 0.454565   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  6 0.682475   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=4 Win=4093 Len=0
  7 0.682581   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  8 0.910513   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=5 Win=4092 Len=0
  9 1.413367   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
 10 1.446812   13.0.0.1   10.0.0.2   TELNET Telnet Data ...
 11 1.572052   10.0.0.2   13.0.0.1   TCP    1186 > telnet [ACK] Seq=7 Ack=10 Win=65465 Len=0
⊞ Frame 3 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 13.0.0.1 (13.0.0.1)
⊞ Transmission Control Protocol, Src Port: 1186 (1186), Dst Port: telnet (23), Seq: 1, Ack: 0, Len: 1
⊟ Telnet
    Data: i
```

```
  1 0.000000   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  2 0.226514   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=1 Win=4096 Len=0
  3 0.226615   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  4 0.454463   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=2 Win=4095 Len=0
  5 0.454565   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  6 0.682475   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=4 Win=4093 Len=0
  7 0.682581   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  8 0.910513   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=5 Win=4092 Len=0
  9 1.413367   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
 10 1.446812   13.0.0.1   10.0.0.2   TELNET Telnet Data ...
 11 1.572052   10.0.0.2   13.0.0.1   TCP    1186 > telnet [ACK] Seq=7 Ack=10 Win=65465 Len=0
⊞ Frame 1 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 13.0.0.1 (13.0.0.1)
⊞ Transmission Control Protocol, Src Port: 1186 (1186), Dst Port: telnet (23), Seq: 0, Ack: 0, Len: 1
⊟ Telnet
    Data: c
```

```
  1 0.000000   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  2 0.226514   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=1 Win=4096 Len=0
  3 0.226615   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  4 0.454463   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=2 Win=4095 Len=0
  5 0.454565   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  6 0.682475   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=4 Win=4093 Len=0
  7 0.682581   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
  8 0.910513   13.0.0.1   10.0.0.2   TCP    telnet > 1186 [ACK] Seq=0 Ack=5 Win=4092 Len=0
  9 1.413367   10.0.0.2   13.0.0.1   TELNET Telnet Data ...
 10 1.446812   13.0.0.1   10.0.0.2   TELNET Telnet Data ...
 11 1.572052   10.0.0.2   13.0.0.1   TCP    1186 > telnet [ACK] Seq=7 Ack=10 Win=65465 Len=0
⊞ Frame 7 (60 bytes on wire, 60 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol, Src: 10.0.0.2 (10.0.0.2), Dst: 13.0.0.1 (13.0.0.1)
⊞ Transmission Control Protocol, Src Port: 1186 (1186), Dst Port: telnet (23), Seq: 4, Ack: 0, Len: 1
⊟ Telnet
    Data: o
```

Fuente. Captura de pantalla Wireshark versión 0.99.5

- Para el escenario 2

Figura 19. Resultados de la prueba 1 para el escenario 2.

```
21 48.604219   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
22 48.857866   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
23 49.060979   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
24 49.314104   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
25 49.427213   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
26 49.677915   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
27 49.678036   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
28 49.774652   fe80::211:92ff:fe6a:7a00              2001:db8:2222:1:101b:6be0:743c:81aa   ICMPv6 Neighbor solicitati
29 49.774717   2001:db8:2222:1:101b:6be0:743c:81aa   fe80::211:92ff:fe6a:7a00              ICMPv6 Neighbor advertisem
30 49.929957   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
31 49.930072   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
32 49.984978   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TELNET Telnet Data ...
33 49.990986   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
⊞ Frame 21 (75 bytes on wire, 75 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol Version 6
⊞ Transmission Control Protocol, Src Port: 1026 (1026), Dst Port: telnet (23), Seq: 32, Ack: 61, Len: 1
⊟ Telnet
    Data: c
```

```
33 49.990986   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
34 50.002593   Cisco_6a:7a:00                        Cisco_6a:7a:00                        LOOP   Reply
35 50.241955   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
36 50.242035   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
37 50.493995   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
38 50.494101   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
39 50.745949   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
⊞ Frame 33 (75 bytes on wire, 75 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol Version 6
⊞ Transmission Control Protocol, Src Port: 1026 (1026), Dst Port: telnet (23), Seq: 38, Ack: 62, Len: 1
⊟ Telnet
    Data: i
```

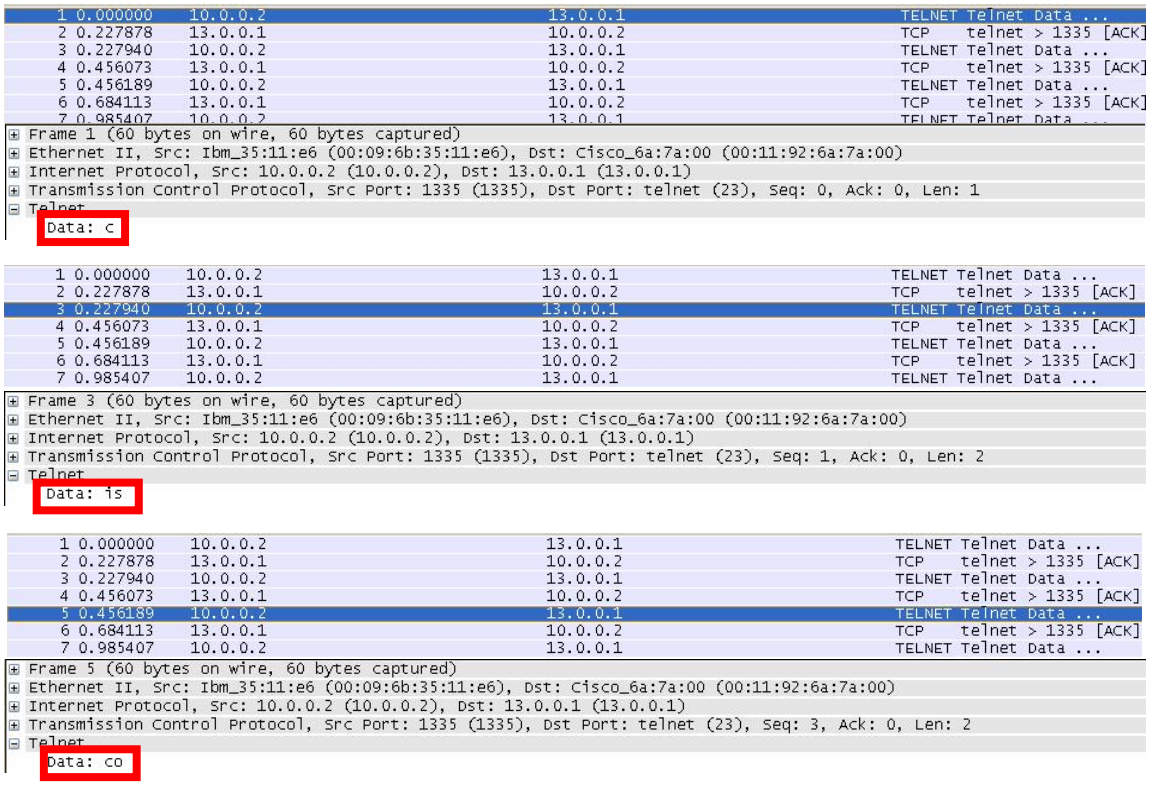
```
33 49.990986   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
34 50.002593   Cisco_6a:7a:00                        Cisco_6a:7a:00                        LOOP   Reply
35 50.241955   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
36 50.242035   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
37 50.493995   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
38 50.494101   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
39 50.745949   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
⊞ Frame 36 (76 bytes on wire, 76 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol Version 6
⊞ Transmission Control Protocol, Src Port: 1026 (1026), Dst Port: telnet (23), Seq: 39, Ack: 62, Len: 2
⊟ Telnet
    Data: sc
```

```
33 49.990986   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
34 50.002593   Cisco_6a:7a:00                        Cisco_6a:7a:00                        LOOP   Reply
35 50.241955   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
36 50.242035   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
37 50.493995   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
38 50.494101   2001:db8:2222:1:101b:6be0:743c:81aa   2001:db8:0:1::                        TELNET Telnet Data ...
39 50.745949   2001:db8:0:1::                        2001:db8:2222:1:101b:6be0:743c:81aa   TCP    telnet > 1026 [ACK]
⊞ Frame 38 (75 bytes on wire, 75 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol Version 6
⊞ Transmission Control Protocol, Src Port: 1026 (1026), Dst Port: telnet (23), Seq: 41, Ack: 62, Len: 1
⊟ Telnet
    Data: o
```

Fuente., Ibíd.

- Para el escenario 3

Figura 20. Resultados de la prueba 1 para el escenario 3.



Fuente., Ibíd.

- Para el escenario 4

Figura 21. Resultados de la prueba 1 para el escenario 4.

```
16 17.748594 Cisco_be:44:d2                    CDP/VTP                                CDP    Cisco Discovery Prot
17 18.689563 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
18 18.929340 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
19 18.929434 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
20 19.169307 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
21 19.169403 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
22 19.409434 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
23 19.409530 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...

⊞ Frame 17 (75 bytes on wire, 75 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol Version 6
⊞ Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: telnet (23), Seq: 32, Ack: 61, Len: 1
⊟ Telnet
    Data: c
```

```
17 18.689563 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
18 18.929340 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
19 18.929434 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
20 19.169307 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
21 19.169403 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
22 19.409434 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
23 19.409530 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...

⊞ Frame 19 (76 bytes on wire, 76 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol Version 6
⊞ Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: telnet (23), Seq: 33, Ack: 61, Len: 2
⊟ Telnet
    Data: is
```

```
17 18.689563 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
18 18.929340 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
19 18.929434 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
20 19.169307 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
21 19.169403 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
22 19.409434 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
23 19.409530 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...

⊞ Frame 21 (75 bytes on wire, 75 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol Version 6
⊞ Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: telnet (23), Seq: 35, Ack: 61, Len: 1
⊟ Telnet
    Data: c
```

```
19 18.929434 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
20 19.169307 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
21 19.169403 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
22 19.409434 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]
23 19.409530 2001:db8:2222:1:dda2:a8f5:7a63:29a5  2001:db8:0:1::                       TELNET Telnet Data ...
24 19.649387 2001:db8:0:1::                    2001:db8:2222:1:dda2:a8f5:7a63:29a5    TCP    telnet > 1027 [ACK]

⊞ Frame 23 (75 bytes on wire, 75 bytes captured)
⊞ Ethernet II, Src: Ibm_35:11:e6 (00:09:6b:35:11:e6), Dst: Cisco_6a:7a:00 (00:11:92:6a:7a:00)
⊞ Internet Protocol Version 6
⊞ Transmission Control Protocol, Src Port: 1027 (1027), Dst Port: telnet (23), Seq: 36, Ack: 61, Len: 1
⊟ Telnet
    Data: o
```

Fuente., Ibíd.

Como se puede observar en los resultados de la prueba uno, implementada sobre cada escenario, la clave viaja por la red en texto plano, sin importar el protocolo IP implementado (ver recuadros en rojo), lo que indica que ningún proceso de autenticación ni de cifrado se llevo a cabo.

4.2 PRUEBA 2

Esta prueba consiste en el envió de trafico ICMP a través de los cuatro escenarios (desde el PC1 al PC3), cabe recalcar que los protocolos de seguridad IP (AH y ESP) han sido habilitados manualmente sobre un sistema operativo Windows XP SP 2 (ver punto 9.2.1). El objetivo de esta prueba es observar como tratan IPSec AH e IPSec ESP los paquetes ICMP cuando son enviados a través de la red. Paralelo al envió del trafico ICMP un sniffer será plantado en el PC receptor del trafico ICMP.

Cada escenario será sometido a 2 pruebas una usando IPSec AH y la otra usando IPSec ESP.

4.2.1 Activación Del IPsec AH e IPsec ESP Sobre Windows XP SP2.

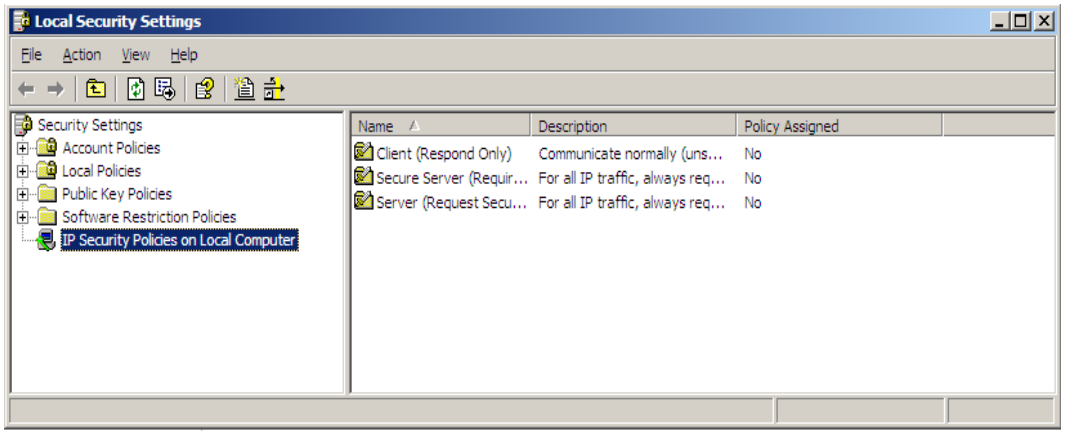
El IPSec para un correcto funcionamiento debe ser activado tanto en el PC que envía el tráfico ICMP como en el PC destino, a continuación se explicara como:

Pasos para la activación de IPSec en el PC destino Del trafico ICMP

- Se selecciona el menú herramientas administrativas a través de Inicio – Panel de control.

- Una vez dentro se da click en la opción Local Security Policy y se despliega la ventana mostrada en la siguiente figura.

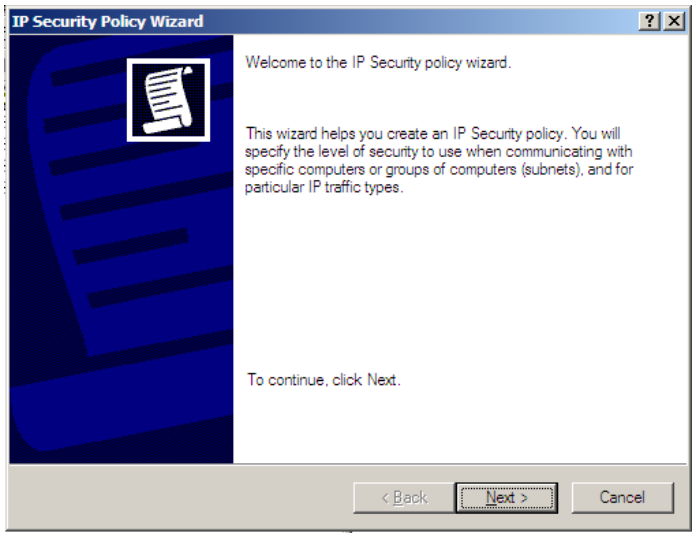
Figura 22. Ventana Local Security Settings.



Fuente. Captura de pantalla Windows XP SP2.

- A continuación se selecciona la opción IP Security on Local Computer. Una vez hecho lo anterior se procederá a crear una nueva política de seguridad IP dando click derecho y seleccionando la opción Create IP Security Policy, el siguiente asistente se despliega.

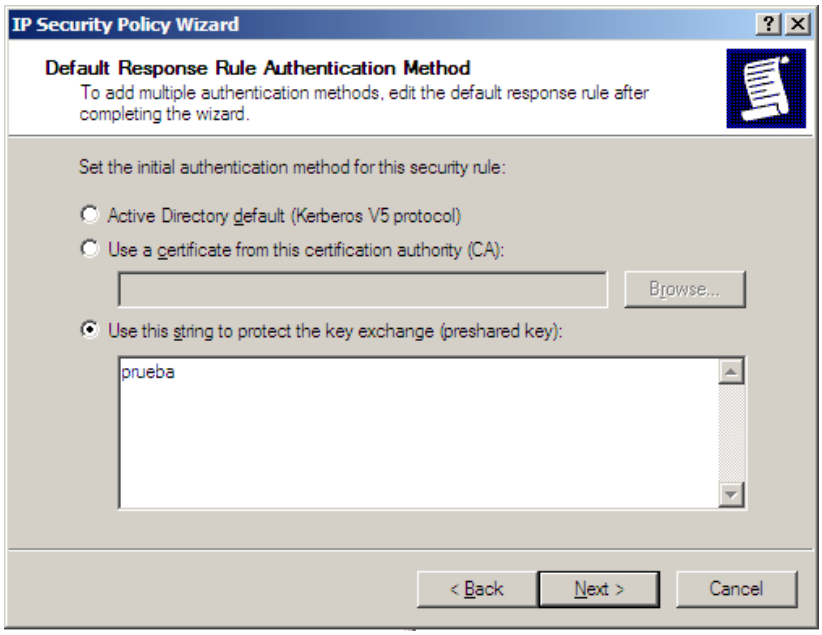
Figura 23. Asistente para la creación de una política de seguridad.



Fuente., Ibíd.

Con el asistente se le define un nombre a la política que va hacer creada, además se selecciona el método de autenticación para los involucrados en la comunicación con IPSec, entre los que se soportan están: Kerberos, CA (Certification Authority) y finalmente el intercambio de llaves o preshared key.

Figura 24. Métodos de autenticación para la política de seguridad.



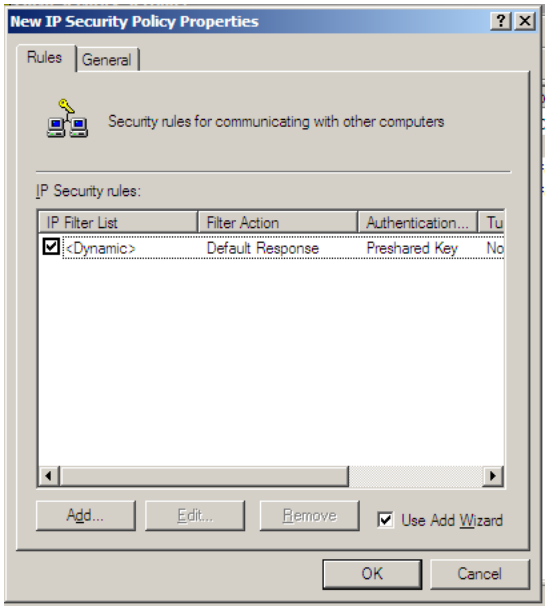
Fuente., Ibíd.

Para esta prueba se selecciona la última opción, la llave que se compartirá para validar la autenticación es la cadena de caracteres “prueba”.

Con este paso se termina la creación de la nueva política de seguridad IP.

- El siguiente paso es la creación de reglas de seguridad IP para la nueva política que ha sido creada, esto se hace dando click sobre el botón Add tal como lo muestra la siguiente figura

Figura 25. Ventana para la creación de reglas de seguridad.

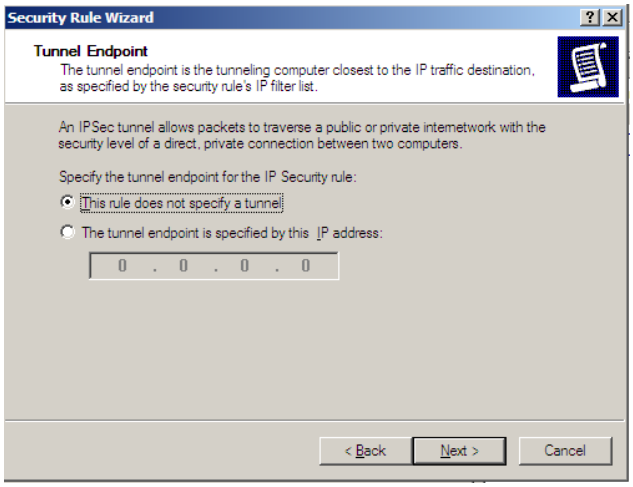


Fuente., Ibíd.

Un asistente aparece y con el se definen los siguientes parámetros:

- Túnel end point: esta opción permite definir una dirección IP destino que será usada para el montaje de un túnel IPSec, el funcionamiento de este tipo de túnel es muy parecido al los que se presentan en las VPN. Para este experimentó se trabajara con IPSec en modo transporte y no en modo túnel por lo tanto se escoge la primera opción.

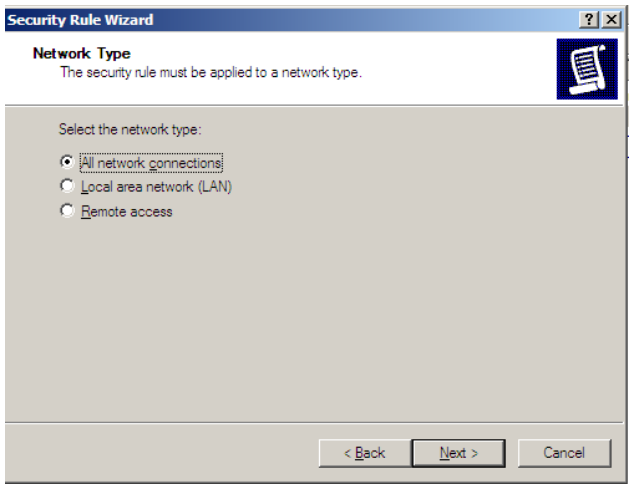
Figura 26. Tunnel End Point.



Fuente., Ibíd.

- La siguiente opción es escoger el tipo de red en el que será usado IPSec, para esta prueba se selecciona la opción All Network Connections.

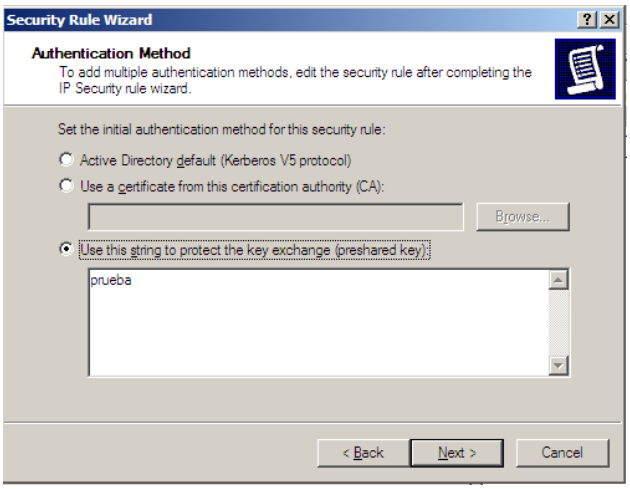
Figura 27. Tipos de red.



Fuente., Ibíd.

- El siguiente parámetro a seleccionar es nuevamente un método de autenticación, al igual como se hizo anteriormente se selecciona el intercambio de llaves o preshared key con la misma cadena de texto “prueba”.

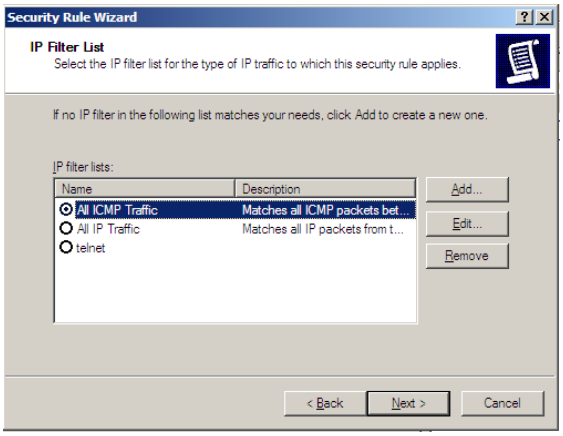
Figura 28. Métodos de autenticación, para la regla de seguridad.



Fuente., Ibíd.

- El siguiente paso es seleccionar un filtro para el trafico (figura 29), este determinara que tipo de trafico será cubierto por IPSec, como se maneja trafico ICMP para este experimento se selecciona el filtro All ICMP Traffic.

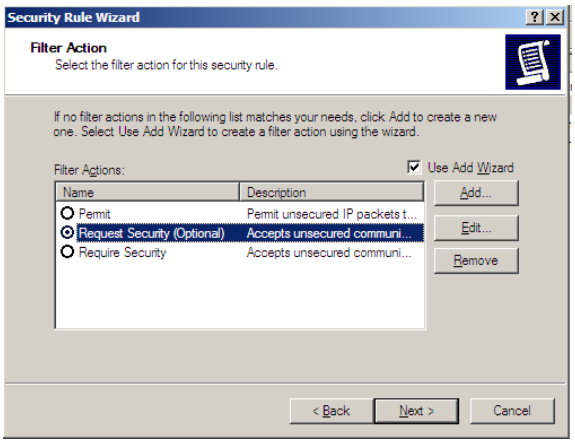
Figura 29. Filtros de tráfico.



Fuente., Ibíd.

- Ahora se selecciona la acción del filtro (figura 30), es decir que tiene que hacer este cuando el tráfico que se selecciono para el filtro llega a una Terminal con IPSec habilitado. Hay 3 opciones: Permit, Require security y Request security. Por propósitos de este experimento se selecciona la opción Request security, con esta, la seguridad será negociada entre el emisor y receptor antes de que cualquier dato sea transmitido.

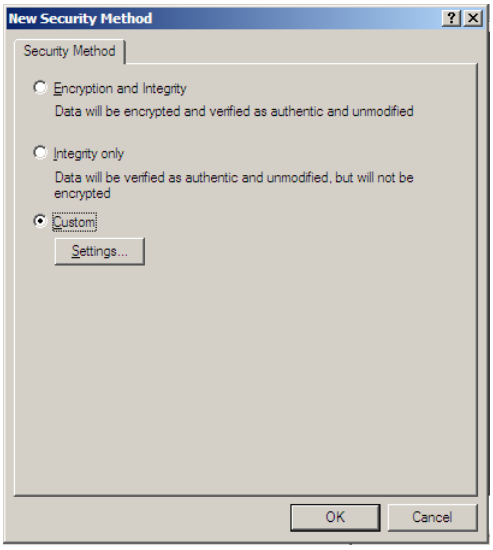
Figura 30. Acción del Filtro de tráfico.



Fuente., Ibíd.

- Al oprimir el botón Edit y luego en la ventana que aparece, se selecciona la opción Add, es posible seleccionar el tipo de IPSec a utilizar (figura 31), ya sea IPSec AH o IPSec ESP.

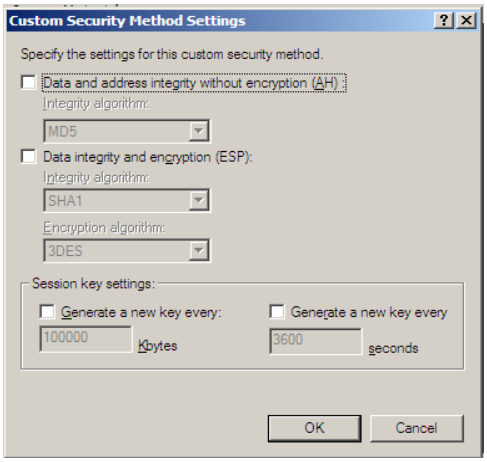
Figura 31. Métodos de seguridad.



Fuente., Ibíd.

Al seleccionar Custom y a continuación la opción Settings es posible aplicar IPSec AH o IPSec ESP según sea necesario (figura 32).

Figura 32. Selección del tipo de encabezado IPSec.



Fuente., Ibíd.

Cabe recordar que IPSec AH brinda sólo autenticación mientras que IPSec ESP brinda autenticación y encripción de datos de extremo a extremo, para tanto AH o ESP se puede usar diferentes algoritmos tales como MD5 (Message-Digest Algorithm 5) y SHA1 (Secure Hash Algorithm 1), para proteger la integridad de los datos o 3DES (3 Data Encryption Standard) y DES (Data Encryption Standard) para la encripción de los datos. Se recomienda el uso de los algoritmos SHA1 y 3DES ya que son los que proporcionan claves más fuertes.

Para este experimento será necesario configurar IPSec ESP e IPSec AH una vez por cada escenario de migración planteado, esto es necesario, para poder ver las diferencias entre los 2 protocolos de seguridad.

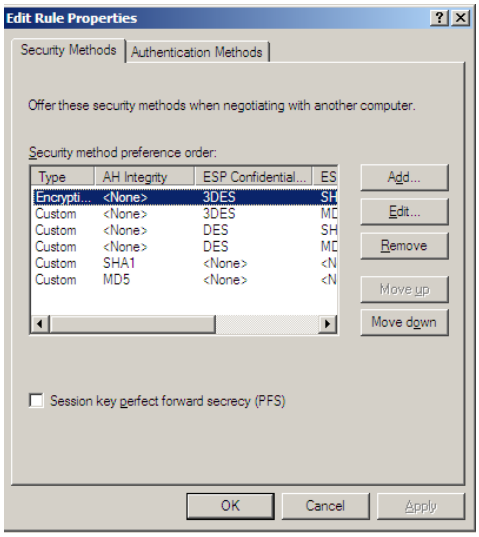
Con este paso se termina la configuración del PC destino.

Pasos para la activación de IPSec en el PC fuente Del trafico ICMP

Para esta configuración los pasos 1, 2 y 3 explicados anteriormente se hacen de igual manera, es partir del paso 4 que las cosas cambian un poco.

En lugar de agregar una nueva regla de seguridad IP, se procederá a editar la que el sistema proporciona por defecto, esto se hace para que se adapte a las condiciones de seguridad que fueron definidas por el receptor del trafico ICMP, esto se hace dando click en el botón Edit, lo que aparece se muestra en la figura 33.

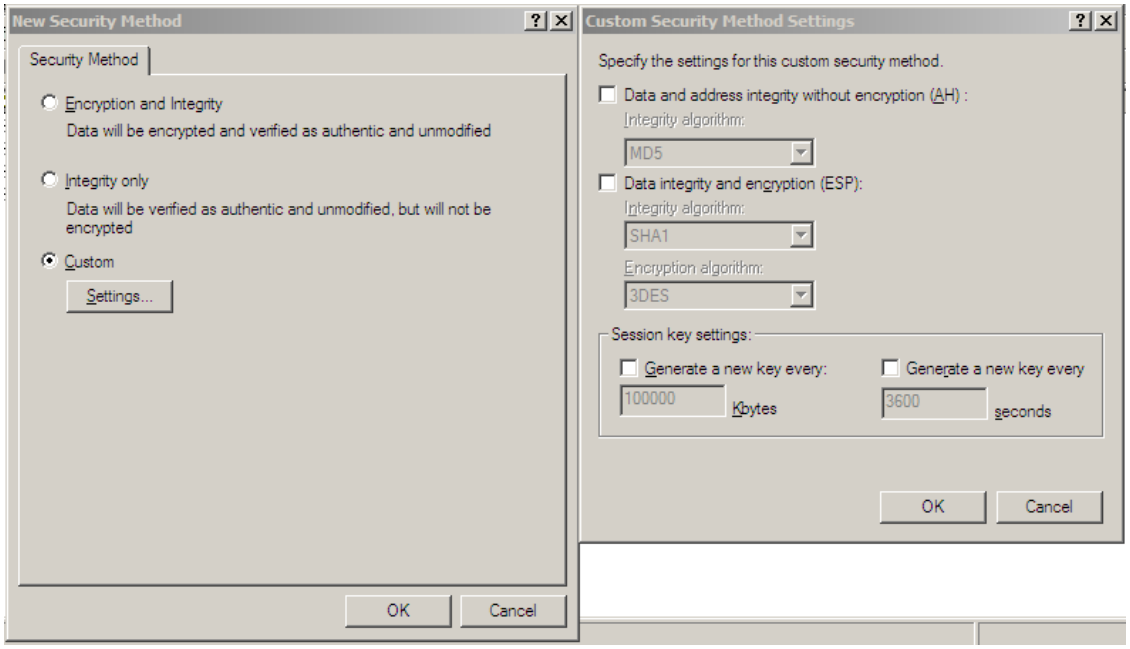
Figura 33. Edición de una política de seguridad.



Fuente., Ibíd.

A continuación, se da click en Add y se selecciona Custom para elegir entre IPSec AH o IPSec ESP, es importante recordar que la configuración escogida en este paso, debe ser igual a la configurada en el PC que recibe el trafico ICMP, si esto no es así el protocolo IPSec no funcionara.

Figura 34. Métodos de seguridad y selección de encabezado IPSec.



Fuente., Ibíd.

Con este paso se culmina la configuración de IPSec sobre un ambiente Windows XP SP2, a continuación se muestran los resultados de la prueba dos.

- Para el escenario 1

Con IPSec AH habilitado

Figura 35. Resultados de la prueba 2, sobre el escenario 1, utilizando IPSec AH.

```
21 14.444729   13.0.0.2    10.0.0.2    ICMP   Echo (ping) request
22 14.444839   10.0.0.2    13.0.0.2    ICMP   Echo (ping) reply
Authentication Header
  Next Header: ICMP (0x01)
  Length: 24
  SPI: 0xa7fead5d
  Sequence: 1
  IV: 5CACE81992045EF4CE963DE9
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x2e5c [correct]
  Identifier: 0x0200
  Sequence number: 7424 (0x1d00)
  Data (32 bytes)
```

Fuente. Captura de pantalla Wireshark versión 0.99.5

Con IPSec ESP habilitado

Figura 36. Resultados de la prueba 2, sobre el escenario 1, utilizando IPSec ESP.

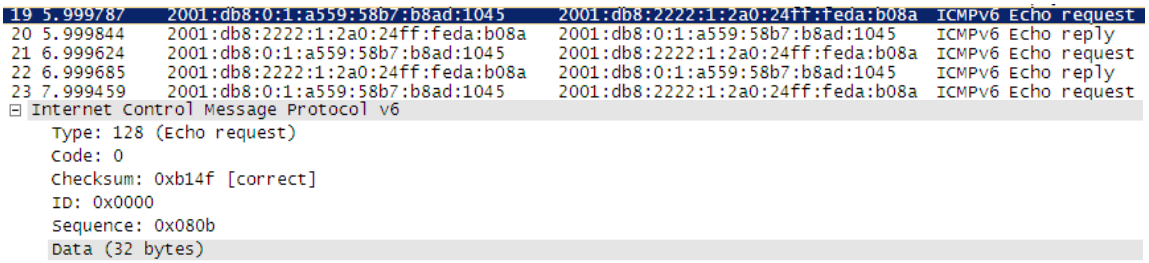
```
3 0.030448    10.0.0.2    13.0.0.2    ESP    ESP (SPI=0x0cafa859)
4 0.858750    13.0.0.2    10.0.0.2    ESP    ESP (SPI=0xabbf8a79)
5 0.858913    10.0.0.2    13.0.0.2    ESP    ESP (SPI=0x0cafa859)
6 1.874094    13.0.0.2    10.0.0.2    ESP    ESP (SPI=0xabbf8a79)
7 1.874255    10.0.0.2    13.0.0.2    ESP    ESP (SPI=0x0cafa859)
8 2.873834    13.0.0.2    10.0.0.2    ESP    ESP (SPI=0xabbf8a79)
⊟ Encapsulating Security Payload
    SPI: 0x0cafa859
    Sequence: 1
```

Fuente., Ibíd.

- Para el escenario 2

Con IPSec AH habilitado

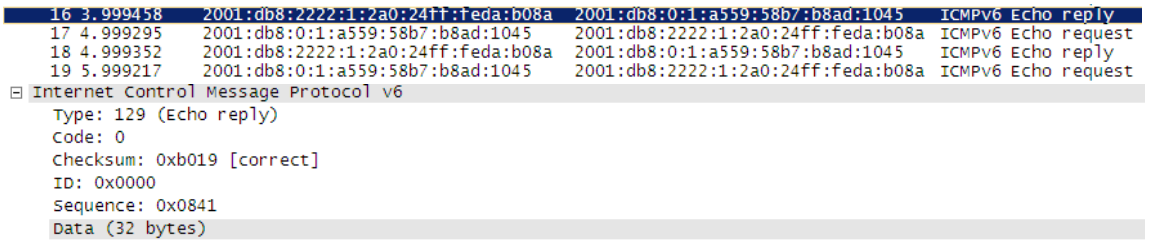
Figura 37. Resultados de la prueba 2, sobre el escenario 2, utilizando IPSec AH.



Fuente., Ibíd.

Con IPSec ESP habilitado

Figura 38. Resultados de la prueba 2, sobre el escenario 2, utilizando IPSec ESP.



Fuente., Ibíd.

- Para el escenario 3

Con IPSec AH habilitado

Figura 39. Resultados de la prueba 2, sobre el escenario 3, utilizando IPSec AH.

```
27 10.921847   10.0.0.2   13.0.0.2   ICMP   Echo (ping) reply
28 11.921653   13.0.0.2   10.0.0.2   ICMP   Echo (ping) request
29 11.921766   10.0.0.2   13.0.0.2   ICMP   Echo (ping) reply
30 12.921576   13.0.0.2   10.0.0.2   ICMP   Echo (ping) request
31 12.921682   10.0.0.2   13.0.0.2   ICMP   Echo (ping) reply
32 13.921412   13.0.0.2   10.0.0.2   ICMP   Echo (ping) request
Authentication Header
  Next Header: ICMP (0x01)
  Length: 24
  SPI: 0x781e3332
  Sequence: 5
  IV: B40DA4ABDEB7969F1326B325
Internet Control Message Protocol
  Type: 0 (Echo (ping) reply)
  Code: 0
  Checksum: 0xe35b [correct]
  Identifier: 0x0200
  Sequence number: 28672 (0x7000)
  Data (32 bytes)
```

Fuente., Ibíd.

Con IPSec ESP habilitado

Figura 40. Resultados de la prueba 2, sobre el escenario 3, utilizando IPSec ESP.

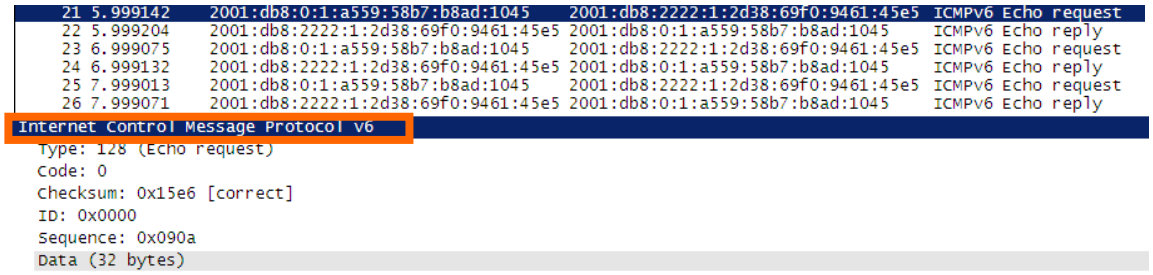
```
30 8.004186   10.0.0.2   13.0.0.2   ESP   ESP (SPI=0x655a7f5d)
31 9.003594   13.0.0.2   10.0.0.2   ESP   ESP (SPI=0xc8e55575)
32 9.003753   10.0.0.2   13.0.0.2   ESP   ESP (SPI=0x655a7f5d)
33 10.003787  13.0.0.2   10.0.0.2   ESP   ESP (SPI=0xc8e55575)
34 10.003944  10.0.0.2   13.0.0.2   ESP   ESP (SPI=0x655a7f5d)
35 11.018944  13.0.0.2   10.0.0.2   ESP   ESP (SPI=0xc8e55575)
Encapsulating Security Payload
  SPI: 0xc8e55575
  Sequence: 2
```

Fuente., Ibíd.

- Para el escenario 4

Con IPSec AH habilitado

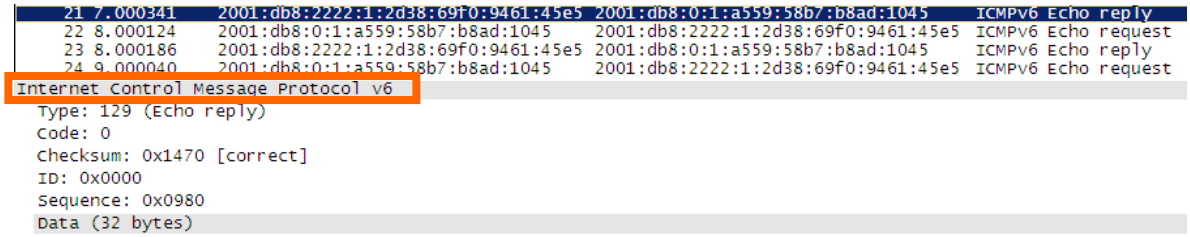
Figura 41. Resultados de la prueba 2, sobre el escenario 4, utilizando IPSec AH.



Fuente., Ibíd.

Con IPSec ESP habilitado

Figura 42. Resultados de la prueba 2, sobre el escenario 4, utilizando IPSec ESP.



Fuente., Ibíd.

Para la prueba dos, la seguridad IP fue manualmente habilitada sobre un ambiente Windows, cada escenario fue probado usando primero IPSec AH y luego IPSec ESP; como se puede observar en los resultados, sobre IPv4, cuando IPSec AH esta habilitado, el emisor y receptor se autentican, pero el contenido del paquete

no se cifra, por lo tanto, si una vez autenticados los extremos, el paquete llega a otro PC ajeno a la comunicación, su contenido será legible (ver recuadros en rojo). Con IPSec ESP no se realiza ningún proceso de autenticación, pero todo paquete es cifrado antes de ser enviado, por consiguiente, aun si el paquete llega a un PC ajeno a la comunicación, su contenido no podrá revisar su contenido a menos de que pueda desencriptar el paquete (ver recuadros en verde). Sobre IPv6 los resultados son diferentes, tanto la autenticación como el cifrado no se realizaron, aun cuando la seguridad fue implementada, el paquete viaja por la red sin ningún tipo de protección (Ver recuadros en naranja).

4.3 PRUEBA 3.

En esta prueba un servidor Web (Apache 2.2.4) fue habilitado sobre un PC con Linux Fedora Core 6, este servidor fue configurado para pedir una contraseña de acceso, que le permitirá al usuario que intente conectarse a el, ver el contenido de una pagina de prueba. Paralelo al ingreso de la clave, el servidor tendrá instalado un sniffer en modo promiscuo, el objetivo de la prueba es tratar de capturar la contraseña configurada en el momento que sea enviada desde el cliente al servidor.

La instalación y configuración del servidor apache se explica a continuación.

4.3.1 Pasos de la Compilación E Instalación Del Servidor Apache En Fedora Core 6.

- Se descarga el archivo http-2.2.4.tar.gz de la página de Apache HTTP SERVER PROJECT. (link http://httpd.apache.org/).

- Luego almacene el archivo en la carpeta /usr/local/apache2, si no existe créela. Paralelo a este paso, cree otra carpeta en la misma ruta llamada Apache, es en esta en donde se hará la compilación e instalación del servidor Web.

- El siguiente paso, es descomprimir el archivo descargado, para esto acceda a la ruta donde esta el archivo (/usr/local/apache2) y digite los siguientes comandos:

```
gzip -d httpd-2.2.4.tar.gz
tar xvf httpd-2.2.4.tar
```

- Por el terminal de comandos de Linux, acceda a la carpeta /usr/local/apache2 y ejecute el siguiente comando: ./configure –prefix=/usr/local/Apache, finalice con enter. Este comando le indica al sistema en donde compilar e instalar el servidor.

- Luego, digite el comando Make, este iniciara la compilación del apache con las opciones por defecto, tenga un poco de paciencia ahora, porque una configuración básica tarda aproximadamente 3 minutos en compilar, pero el tiempo puede variar dependiendo de las características del PC que se este utilizando.

- Luego de terminada la compilación se procede a la instalación, este paso se realiza con el comando Make install, al igual que la compilación, la instalación puede llevar algo de tiempo, tenga paciencia.

Con este paso se termina la compilación e instalación, lo siguiente es configurar el servidor para que pida una clave de acceso.

4.3.2 Configuración Del Servidor Apache

- El primer paso para la configuración de una clave de acceso, es crear el archivo que contenga el usuario y la contraseña de acceso, este se hace desde el terminal de comandos de Linux, accediendo a la carpeta /usr/local/Apache/bin y ejecutando el comando htpasswd –c Nombre del archivo username (ejemplo: htpasswd –c password prueba). Luego de este paso se le va a pedir al usuario que ingrese una contraseña para esta prueba se uso la palabra cisco.

- El siguiente paso es editar el archivo de configuración del apache httpd.conf (usando cualquier procesador de texto disponible), para que solicite la contraseña, al usuario que este agregado en el archivo de contraseñas. El archivo de configuración esta almacenado en la ruta: /etc/httpd/conf.

  En el archivo de configuración se deben digitar las siguientes instrucciones:

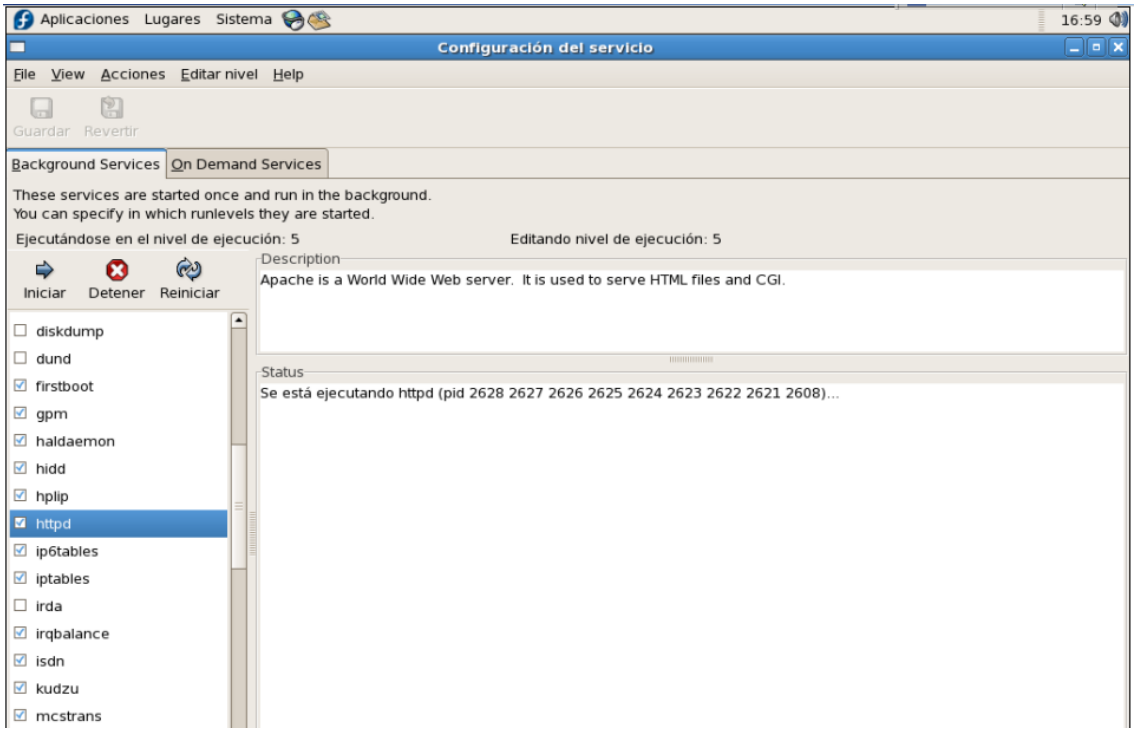
  ```
  <Directory “/var/www/html”>
  AuthType Basic
  AuthName "Area restringida"
  AuthBasicProvider file
  AuthUserFile "/usr/local/Apache/bin/password”
  Require user prueba
  </Directory>
  ```

- Es importante recordar que el apache por defecto no recibe solicitudes IPv6, entonces es necesario configurarlo, esto se hace sobre el mismo archivo httpd.conf , agregando las líneas:

  ```
  Listen [::]:80
  Listen 81
  ```

- El paso final es iniciar el servidor esto se puede hacer de dos maneras:
  - La primera manera, es por modo comando, ingresar la ruta /usr/local/Apache/bin y digitar el comando apachectl start (para iniciar el servidor) o apachectl stop (para detenerlo).
  - La segunda manera es desde la ventana de servicios de Linux Fedora Core 6. Se accede a ella desde el menú Sistema – Administración – Services. Una vez dentro se debe buscar un servicio llamado httpd y dar sobre el botón iniciar de la parte superior de la lista para iniciar el servidor. Tal como se muestra en la figura

Figura 43. Ventana de servicios de Linux Fedora Core 6.



Fuente. Captura de pantalla Linux Fedora Core 6.

Con este paso se culmina la configuración del servidor Apache, a continuación se muestran los resultados de la prueba tres.

4.3.3 Resultados De La Prueba 3

- Para el escenario 1

Figura 44. Resultados de la prueba 3, sobre el escenario 1.

Source	Destination	Protocol	Info
10.0.0.2	13.0.0.2	HTTP	GET / HTTP/1.1
13.0.0.2	10.0.0.2	TCP	http > 1136 [ACK] Seq=1 Ack=345 Win=6432 Len=0
13.0.0.2	10.0.0.2	HTTP	HTTP/1.1 200 OK (text/html)
13.0.0.2	10.0.0.2	TCP	http > 1136 [FIN, ACK] Seq=307 Ack=345 Win=6432 Len=0
10.0.0.2	13.0.0.2	TCP	1136 > http [FIN, ACK] Seq=345 Ack=307 Win=65229 Len=0
13.0.0.2	10.0.0.2	TCP	http > 1136 [ACK] Seq=308 Ack=346 Win=6432 Len=0
10.0.0.2	13.0.0.2	TCP	1136 > http [ACK] Seq=346 Ack=308 Win=65229 Len=0
10.0.0.2	13.0.0.2	TCP	1137 > http [SYN] Seq=0 Len=0 MSS=1460
13.0.0.2	10.0.0.2	TCP	http > 1137 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
10.0.0.2	13.0.0.2	TCP	1137 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
10.0.0.2	13.0.0.2	HTTP	GET /favicon.ico HTTP/1.1
13.0.0.2	10.0.0.2	TCP	http > 1137 [ACK] Seq=1 Ack=231 Win=6432 Len=0
13.0.0.2	10.0.0.2	HTTP	HTTP/1.1 404 Not Found (text/html)
13.0.0.2	10.0.0.2	TCP	http > 1137 [FIN, ACK] Seq=462 Ack=231 Win=6432 Len=0
10.0.0.2	13.0.0.2	TCP	1137 > http [FIN, ACK] Seq=231 Ack=462 Win=65074 Len=0
13.0.0.2	10.0.0.2	TCP	http > 1137 [ACK] Seq=463 Ack=232 Win=6432 Len=0
10.0.0.2	13.0.0.2	TCP	1137 > http [ACK] Seq=232 Ack=463 Win=65074 Len=0

```
⊟ Hypertext Transfer Protocol
  ⊞ GET /favicon.ico HTTP/1.1\r\n
    Accept: */*\r\n
    UA-CPU: x86\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)\r\n
    Host: 13.0.0.2\r\n
    Connection: Keep-Alive\r\n
  ⊟ Authorization: Basic cHJ1ZWJhOmNpc2Nv\r\n
      Credentials: prueba:cisco
    \r\n
```

Fuente. Captura de pantalla Wireshark versión 0.99.5

- Para el escenario 2

Figura 45. Resultados de la prueba 3, sobre el escenario 2.

Source	Destination	Protocol	Info
2001:db8:2222:1:e5e4:22b:36d7:f31c	2001:db8:0:1:209:6bff:fe35:156b	TCP	1025 > http [FIN, ACK] Seq=331 Ack=741 Win=16541 L
2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:e5e4:22b:36d7:f31c	TCP	http > 1025 [ACK] Seq=741 Ack=332 Win=6432 Len=0
2001:db8:2222:1:e5e4:22b:36d7:f31c	2001:db8:0:1:209:6bff:fe35:156b	TCP	1026 > http [SYN] Seq=0 Len=0 MSS=1440
2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:e5e4:22b:36d7:f31c	TCP	http > 1026 [SYN, ACK] Seq=0 Ack=1 Win=5760 Len=0
2001:db8:2222:1:e5e4:22b:36d7:f31c	2001:db8:0:1:209:6bff:fe35:156b	TCP	1026 > http [ACK] Seq=1 Ack=1 Win=17280 Len=0
2001:db8:2222:1:e5e4:22b:36d7:f31c	2001:db8:0:1:209:6bff:fe35:156b	HTTP	GET / HTTP/1.1
2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:e5e4:22b:36d7:f31c	TCP	http > 1026 [ACK] Seq=1 Ack=370 Win=6432 Len=0
2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:e5e4:22b:36d7:f31c	HTTP	HTTP/1.1 200 OK (text/html)
2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:e5e4:22b:36d7:f31c	TCP	http > 1026 [FIN, ACK] Seq=307 Ack=370 Win=6432 Le
2001:db8:2222:1:e5e4:22b:36d7:f31c	2001:db8:0:1:209:6bff:fe35:156b	TCP	1026 > http [FIN, ACK] Seq=370 Ack=307 Win=16974 L
2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:e5e4:22b:36d7:f31c	TCP	http > 1026 [ACK] Seq=308 Ack=371 Win=6432 Len=0
2001:db8:2222:1:e5e4:22b:36d7:f31c	2001:db8:0:1:209:6bff:fe35:156b	TCP	1026 > http [ACK] Seq=371 Ack=308 Win=16974 Len=0

```
⊟ Hypertext Transfer Protocol
  ⊞ GET / HTTP/1.1\r\n
    Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword,
    Accept-Language: es\r\n
    UA-CPU: x86\r\n
    Accept-Encoding: gzip, deflate\r\n
    User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)\r\n
    Host: [2001:db8:0:1:209:6bff:fe35:156b]\r\n
    Connection: Keep-Alive\r\n
  ⊟ Authorization: Basic cHJ1ZWJhOmNpc2Nv\r\n
      Credentials: prueba:cisco
    \r\n
```

Fuente. Captura de pantalla Wireshark versión 0.99.5

- Para el escenario 3

Usando IPv4

Figura 46. Resultados de la prueba 3, sobre el escenario 3, usando IPv4.

```
13.0.0.2    10.0.0.2    TCP   http > 1266 [ACK] Seq=718 Ack=307 Win=6432 Len=0
10.0.0.2    13.0.0.2    TCP   1267 > http [SYN] Seq=0 Len=0 MSS=1460
13.0.0.2    10.0.0.2    TCP   http > 1267 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
10.0.0.2    13.0.0.2    TCP   1267 > http [ACK] Seq=1 Ack=1 Win=65535 Len=0
10.0.0.2    13.0.0.2    HTTP  GET / HTTP/1.1
13.0.0.2    10.0.0.2    TCP   http > 1267 [ACK] Seq=1 Ack=345 Win=6432 Len=0
13.0.0.2    10.0.0.2    HTTP  HTTP/1.1 200 OK (text/html)
13.0.0.2    10.0.0.2    TCP   http > 1267 [FIN, ACK] Seq=307 Ack=345 Win=6432 Len=0
10.0.0.2    13.0.0.2    TCP   1267 > http [FIN, ACK] Seq=345 Ack=307 Win=65229 Len=0
Hypertext Transfer Protocol
⊞ GET / HTTP/1.1\r\n
  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword,
  Accept-Language: es\r\n
  UA-CPU: x86\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)\r\n
  Host: 13.0.0.2\r\n
  Connection: Keep-Alive\r\n
⊟ Authorization: Basic cHJ1ZWJhOmNpc2Nv\r\n
    Credentials: prueba:cisco
  \r\n
```

Fuente. Captura de pantalla Wireshark versión 0.99.5 Usando IPv6

Figura 47. Resultados de la prueba 3, sobre el escenario 3, usando IPv6.

```
2001:db8:2222:1:84e4:595e:bbf9:6554  2001:db8:0:1:209:6bff:fe35:156b      TCP   1029 > http [SYN] Seq=0 Len=0 MSS=1440
2001:db8:0:1:209:6bff:fe35:156b      2001:db8:2222:1:84e4:595e:bbf9:6554  TCP   http > 1029 [SYN, ACK] Seq=0 Ack=1 Win=5760 Len=
2001:db8:2222:1:84e4:595e:bbf9:6554  2001:db8:0:1:209:6bff:fe35:156b      TCP   1029 > http [ACK] Seq=1 Ack=1 Win=17280 Len=0
2001:db8:2222:1:84e4:595e:bbf9:6554  2001:db8:0:1:209:6bff:fe35:156b      HTTP  GET / HTTP/1.1
2001:db8:0:1:209:6bff:fe35:156b      2001:db8:2222:1:84e4:595e:bbf9:6554  TCP   http > 1029 [ACK] Seq=1 Ack=370 Win=6432 Len=0
2001:db8:0:1:209:6bff:fe35:156b      2001:db8:2222:1:84e4:595e:bbf9:6554  HTTP  HTTP/1.1 200 OK (text/html)
2001:db8:0:1:209:6bff:fe35:156b      2001:db8:2222:1:84e4:595e:bbf9:6554  TCP   http > 1029 [FIN, ACK] Seq=307 Ack=370 Win=6432
2001:db8:2222:1:84e4:595e:bbf9:6554  2001:db8:0:1:209:6bff:fe35:156b      TCP   1029 > http [FIN, ACK] Seq=370 Ack=307 Win=1697
Hypertext Transfer Protocol
⊞ GET / HTTP/1.1\r\n
  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword,
  Accept-Language: es\r\n
  UA-CPU: x86\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)\r\n
  Host: [2001:db8:0:1:209:6bff:fe35:156b]\r\n
  Connection: Keep-Alive\r\n
⊟ Authorization: Basic cHJ1ZWJhOmNpc2Nv\r\n
    Credentials: prueba:cisco
```

Fuente. Captura de pantalla Wireshark versión 0.99.5

- Para el escenario 4

Figura 48. Resultados de la prueba 3, sobre el escenario 4.

```
2001:db8:2222:1:4878:900a:2de2:e112  2001:db8:0:1:209:6bff:fe35:156b     TCP   1032 > http [SYN] Seq=0 Len=0 MSS=1440
2001:db8:0:1:209:6bff:fe35:156b      2001:db8:2222:1:4878:900a:2de2:e112 TCP   http > 1032 [SYN, ACK] Seq=0 Ack=1 Win=
2001:db8:2222:1:4878:900a:2de2:e112  2001:db8:0:1:209:6bff:fe35:156b     TCP   1032 > http [ACK] Seq=1 Ack=1 Win=1728(
2001:db8:2222:1:4878:900a:2de2:e112  2001:db8:0:1:209:6bff:fe35:156b     HTTP  GET / HTTP/1.1
2001:db8:0:1:209:6bff:fe35:156b      2001:db8:2222:1:4878:900a:2de2:e112 TCP   http > 1032 [ACK] Seq=1 Ack=370 Win=64:
2001:db8:0:1:209:6bff:fe35:156b      2001:db8:2222:1:4878:900a:2de2:e112 HTTP  HTTP/1.1 200 OK (text/html)
2001:db8:0:1:209:6bff:fe35:156b      2001:db8:2222:1:4878:900a:2de2:e112 TCP   http > 1032 [FIN, ACK] Seq=307 Ack=370
Hypertext Transfer Protocol
⊞ GET / HTTP/1.1\r\n
  Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-shockwave-flash, application/msword,
  Accept-Language: es\r\n
  UA-CPU: x86\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1)\r\n
  Host: [2001:db8:0:1:209:6bff:fe35:156b]\r\n
  Connection: Keep-Alive\r\n
⊟ Authorization: Basic cHJ1ZWJhOmNpc2Nv\r\n
    Credentials: prueba:cisco
```

Fuente., Ibíd.

Para la prueba tres, como se puede observar en los resultados, el nombre de usuario y la clave, requeridos para la conexión al servidor, viajan por la red en texto plano sin importar el protocolo IP implementado (Ver recuadros en rojo), lo que indica que ningún proceso de autenticación, ni de cifrado se llevo acabo.

4.4 PRUEBA 4.

Para esta prueba un servidor Web (Apache 2.2.4) fue habilitado sobre un PC con Linux Fedora Core 6, este servidor fue configurado para pedir una contraseña de acceso, que le permitirá al usuario que intente conectarse a el, ver el contenido de una pagina de prueba. Paralelo al ingreso de la clave el servidor tendrá instalado un sniffer en modo promiscuo, el objetivo de la prueba es tratar de capturar la

contraseña configurada en el momento que sea enviada desde el cliente al servidor.

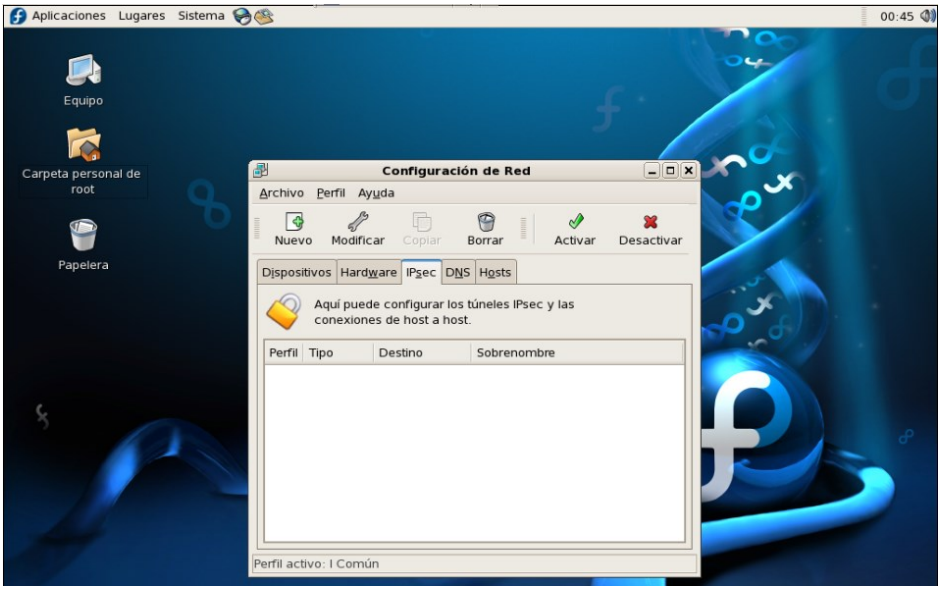
Para esta prueba los protocolos de seguridad IP fueron activados manualmente sobre el sistema operativo Linux Fedora Core 6, la activación y configuración se muestra a continuación.

4.4.1 Activación Del Ipsec Sobre Linux Fedora Core 6. IPSec sobre Linux funciona solo en modo túnel por lo tanto para que entre en funcionamiento y exista una comunicación bidireccional, la configuración debe realizarse tanto en el PC fuente como en el destino. Los pasos para activar IPSec son:

- Se entra en el menú Sistema, luego en el menú Administration y de la lista que se despliega se selecciona la opción Red.

- En la siguiente figura se muestra el menú de configuración de red, estando allí se selecciona la pestaña que dice IPSec. Tal como se muestra en la figura 49.

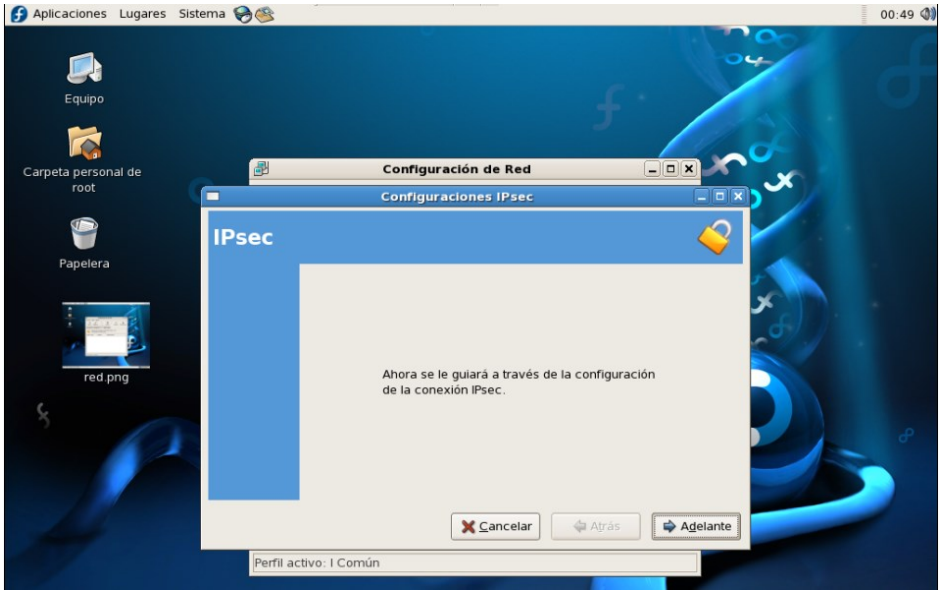
Figura 49. Ventana de configuración de red.



Fuente. Captura de pantalla Linux Fedora Core 6.

- Ubicados sobre el menú IPSec, se procederá a activar la seguridad, para esto, seleccionamos la opción Nuevo. Una ventana de configuración se despliega.

Figura 50. Asistente para la configuración de IPSec.



Fuente., Ibíd.

- En la ventana de configuración se presiona el botón Adelante, el asistente procederá a preguntar una serie de datos, que deben ser configurados para habilitar el IPSec en una conexión.

- El primer dato que se solicita es un sobrenombre para la conexión IPSec, el usuario es libre para seleccionar el que desee.

Figura 51. Sobrenombre para la conexión IPSec.

Fuente., Ibíd.

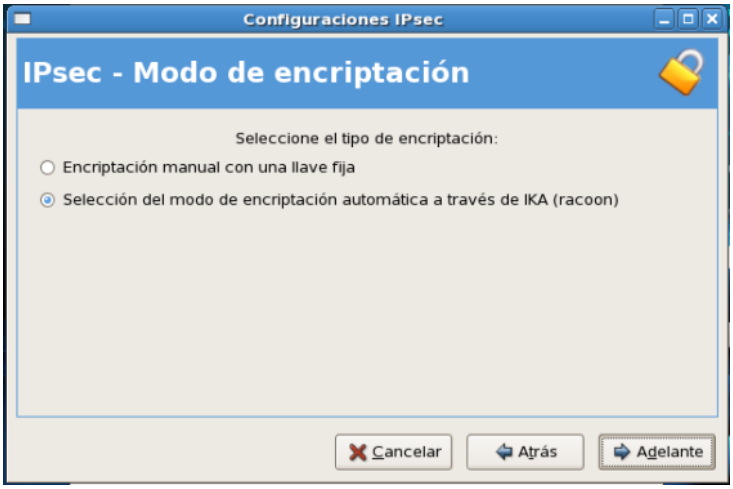
- Lo siguiente a configurar es el tipo de conexión a realizar, existen 2 tipos: Host a Host o Red a Red, la elección debe hacerse de acuerdo a los requerimientos de seguridad que se desean configurar y de acuerdo al ambiente que se desea proteger, por ejemplo si solo se desea proteger la conexión entre un cliente y un servidor se selecciona de Host a Host, pero si se desea proteger toda una red se selecciona la opción de Red a Red, esta opción funciona tal como si fuera una VPN (Virtual Private Network), es decir crea un túnel entre una red y otra, en el cual todo trafico que sea enviado esta protegido con IPSec, se recomienda su uso cuando se accede a la red interna de una empresa (intranet). Para esta prueba se selecciona la opción de Host a Host, tal como se muestra en la figura:

Figura 52. Tipo de conexión.

Fuente., Ibíd.

- El siguiente paso en la configuración es la selección del modo de encripción, esto le permite al usuario escoger la manera en que se desea generar y compartir las llaves de autenticación entre los host, el usuario puede escoger entre: Encriptación manual con una llave fija o Encripción automática a través de IKA (racoon). Con encripción manual todo el proceso lo configura el usuario, es decir debe indicar la forma en que desea que se compartan las llaves y además debe generar por si mismo la llave a compartir, con la segunda opción, el protocolo racoon se encarga de generar la llave y compartirla entre los host implicados. Para esta prueba seleccionamos la opción numero dos, tal como se muestra en la figura:

Figura 53. Modo de encriptación.



Fuente., Ibíd.

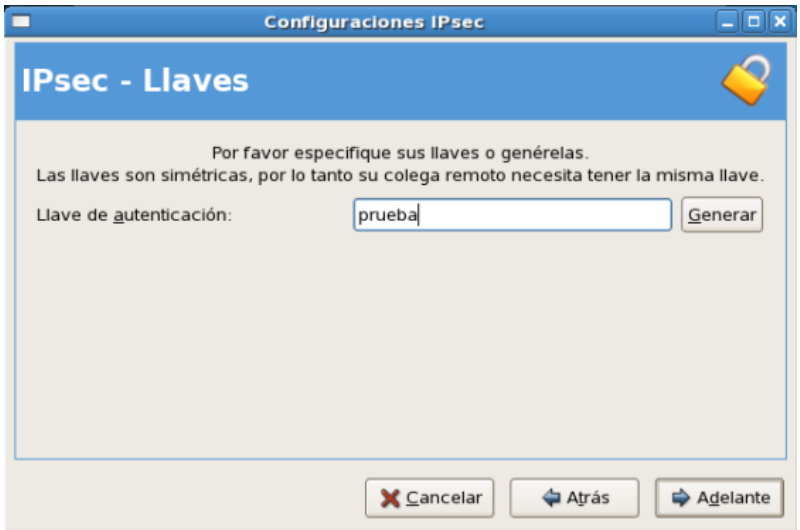
- Ya que se selecciono como tipo de red Host a Host, el paso a seguir es indicar la dirección del host destino, esta dirección se usara para denotar cual es el destino del túnel, se puede especificar una dirección tanto IPv4 como IPv6 según sea necesario.

Figura 54. Red remota.

Fuente., Ibíd.

- El paso final es especificar la cadena de texto que será usada para generar la llave de autenticación, para este caso la cadena es: prueba, tal como se muestra en la figura. El protocolo racoon a partir de esta cadena de texto genera la llave y la intercambia entre los host.

Figura 55. Creación de llaves.



Fuente., Ibíd.

Con este paso se finaliza la configuración de IPSec en el PC fuente.

Los pasos requeridos son exactamente iguales a los ya anteriormente explicados, la única diferencia radica en la definición de la dirección IP del host remoto (paso 8), es decir si se configura el túnel desde el cliente a un servidor, la dirección IP remota es la del servidor, en caso contrario, si se configura el túnel desde el servidor al cliente, la dirección IP remota es la del cliente.

Con este paso se termina la configuración de IPSec, a continuación se muestran los resultados de la prueba 4.

4.4.2 Resultados De La Prueba 4

- Para el escenario 1

Figura 56. Resultados de la prueba 4, sobre el escenario 1.

19	51.900095	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)
20	51.900254	13.0.0.2	10.0.0.2	ESP	ESP (SPI=0x021a0c9a)
21	51.973157	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)
22	52.116198	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)
23	52.116419	13.0.0.2	10.0.0.2	ESP	ESP (SPI=0x021a0c9a)
24	52.117071	13.0.0.2	10.0.0.2	ESP	ESP (SPI=0x021a0c9a)
25	52.117129	13.0.0.2	10.0.0.2	ESP	ESP (SPI=0x021a0c9a)
26	52.410906	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)
27	52.428155	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)

```
⊟ Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x0ab93cee
    Sequence: 1
    IV: 315DDD3534B321D014BDC3B3
⊟ Encapsulating Security Payload
    SPI: 0x03162849
    Sequence: 1
```

Fuente. Captura de pantalla Wireshark versión 0.99.5.

- Para el escenario 2

Figura 57. Resultados de la prueba 4, sobre el escenario 2.

35	56.621336	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
36	56.644462	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)
37	56.709567	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)
38	56.709689	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
39	56.808247	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)
40	56.955070	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)
41	56.955287	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
42	56.956794	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
43	56.956843	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
44	57.213845	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)

```
⊞ Internet Protocol Version 6
⊟ Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x0542be72
    Sequence: 100
    IV: 1CACFE606E5D43A2F60ACF0F
⊟ Encapsulating Security Payload
    SPI: 0x078fed71
    Sequence: 100
```

Fuente., Ibíd.

- Para el escenario 3

Figura 58. Resultados de la prueba 4, sobre el escenario 3.

30	86.164578	13.0.0.2	10.0.0.2	ESP	ESP (SPI=0x021a0c9a)
31	86.237528	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)
32	86.380592	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)
33	86.380803	13.0.0.2	10.0.0.2	ESP	ESP (SPI=0x021a0c9a)
34	86.381442	13.0.0.2	10.0.0.2	ESP	ESP (SPI=0x021a0c9a)
35	86.381499	13.0.0.2	10.0.0.2	ESP	ESP (SPI=0x021a0c9a)
36	86.675271	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)
37	86.692608	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)
38	86.692720	13.0.0.2	10.0.0.2	ESP	ESP (SPI=0x021a0c9a)
39	86.709879	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)
40	91.714898	10.0.0.2	13.0.0.2	ESP	ESP (SPI=0x03162849)

```
⊟ Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x0bad0bbd
    Sequence: 11
    IV: 3093A80356FCBAEF4FA14C60
⊟ Encapsulating Security Payload
    SPI: 0x021a0c9a
    Sequence: 11
```

Fuente., Ibíd.

- Para el escenario 4

Figura 59. Resultados de la prueba 4, sobre el escenario 4.

56	195.005111	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)
57	195.005351	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
58	195.008250	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
59	195.008358	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
60	195.197814	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)
61	195.218130	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)
62	195.218237	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
63	195.238557	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)
64	195.318906	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)
65	195.319038	2001:db8:0:1:209:6bff:fe35:156b	2001:db8:2222:1:20d:60ff:feef:956b	ESP	ESP (SPI=0x078fed71)
66	195.405932	2001:db8:2222:1:20d:60ff:feef:956b	2001:db8:0:1:209:6bff:fe35:156b	ESP	ESP (SPI=0x064b6f89)

```
⊞ Internet Protocol Version 6
⊟ Authentication Header
    Next Header: ESP (0x32)
    Length: 24
    SPI: 0x00e5c8c3
    Sequence: 140
    IV: 9293C7799CCE7A241ADE627B
⊟ Encapsulating Security Payload
    SPI: 0x064b6f89
    Sequence: 140
```

Fuente., Ibíd.

Para la prueba cuatro la seguridad IP fue habilitada manualmente sobre un ambiente Linux, como se puede observar en los resultados, tanto para IPv4 como IPv6, se llevo a cabo la autenticación y cifrado de los paquetes (ver recuadros en rojo), por lo tanto aun cuando el paquete caiga en manos de extraños dado que el proceso de autenticación sea exitoso, su contenido será ilegible.

5. SÍNTESIS DE RESULTADOS

En la tabla mostrada a continuación, se consignan los resultados obtenidos por cada escenario sobre cada una de las pruebas implementadas.

Tabla 2. Tabla comparativa de resultados.

PRUEBA 1								
	Protocolo IP implementado	Trafico involucrado	IPSec habilitado	Resultados con IPSec AH	Resultados con IPSec ESP	Resultados con IPSec desactivado	Autenticación / Confidencialidad *	
Escenario 1	IPv4	Telnet	No	-	-	Contraseña visible	No/No	
	IPv6							
Escenario 2	IPv4	Telnet	No	-	-	Contraseña visible	No/No	
	IPv6							
Escenario 3	IPv4	Telnet	No	-	-	Contraseña visible	No/No	
	IPv6							
Escenario 4	IPv4	Telnet	No	-	-	Contraseña visible	No/No	
	IPv6							
PRUEBA 2								
Escenario 1	IPv4	ICMP	Si	Contenido del paquete visible	Contenido del paquete no visible	-	Si/No	No/Si
	IPv6			-	-		-	-

Escenario 2	IPv4	ICMP	Si	-	-	-	-	-
	IPv6			Contenido del paquete visible	Contenido del paquete visible		No/No	No/No
Escenario 3	IPv4	ICMP	Si	Contenido del paquete visible	Contenido del paquete no visible	-	Si/No	No/Si
	IPv6			Contenido del paquete visible	Contenido del paquete visible		No/No	No/No
Escenario 4	IPv4	ICMP	Si	-	-	-	-	-
	IPv6			Contenido del paquete visible	Contenido del paquete visible		No/No	No/No
PRUEBA 3								
Escenario 1	IPv4	TCP, HTTP	No	-	-	Username y contraseña visibles	No/No	
	IPv6							
Escenario 2	IPv4	TCP, HTTP	No	-	-	Username y contraseña visibles	No/No	
	IPv6							
Escenario 3	IPv4	TCP, HTTP	No	-	-	Username y contraseña visibles	No/No	
	IPv6							
Escenario 4	IPv4	TCP, HTTP	No	-	-	Username y contraseña visibles	No/No	
	IPv6							
PRUEBA 4								
Escenario	IPv4	TCP, HTTP	Si	Username y	Username y	-	Si / Si	Si /

1				contraseña no visibles	contraseña no visibles			Si
	IPv6			-	-		-	-
Escenario 2	IPv4	TCP, HTTP	Si	-	-	-	-	-
	IPv6			Username y contraseña no visibles	Username y contraseña no visibles		Si / Si	Si / Si
Escenario 3	IPv4	TCP, HTTP	Si	Username y contraseña no visibles	Username y contraseña no visibles	-	Si / Si	Si / Si
	IPv6							
Escenario 4	IPv4	TCP, HTTP	Si	-	-	-	-	-
	IPv6			Username y contraseña no visibles	Username y contraseña no visibles		Si / Si	Si / Si

Fuente. Autores del proyecto.

- Las columnas divididas en dos, indican la Autenticación / Confidencialidad, usando IPSec AH o IPSec ESP

6. CONCLUSIONES

Para el desarrollo de esta tesis se utilizaron dos estrategias para la implementación de IPv6, los Túneles Configurados y Dual Snack:

- El uso de túneles configurados para las implementaciones de IPv6 es complejo y poco ventajoso, debido a que es necesario identificar, con precisión, la fuente y el destino del túnel. Además, un túnel sólo permite el envió de información en un sentido, por lo tanto para la comunicación bidireccional es necesario configurar uno de ida y uno de regreso. Este requerimiento convierte a los túneles configurados, en una técnica poco escalable, porque existe una relación, directamente proporcional, entre el número de redes que se pueden conectar y el número de túneles que son necesarios configurar.

- El uso de la técnica Dual Stack es recomendable para una futura migración de IPv4 a IPv6, debido a que permite el manejo simultaneo de ambos estándares, lo que hace posible, la coexistencia de aplicaciones que usan tanto IPv4 como IPv6, además, para su configuración, sólo se requieren conocimientos básicos sobre la arquitectura, esquemas de direccionamiento y protocolos de enrutamiento.

De acuerdo con los resultados obtenidos en las pruebas diseñadas y, posteriormente, implementadas en cada uno de los escenarios de migración propuestos y teniendo como fin principal medir el desempeño de cada uno en materia de seguridad se llegó a la siguiente conclusión:

- La primera y tercera prueba, evidenciaron que sin importar el protocolo IP implementado y tipo de tráfico enviado (TCP, UDP, HTTP, ICMP, Telnet), todo paquete se envía sin ser encriptado y sin realizarse ningún proceso de autenticación, aun cuando en los encabezados IPv6, los estándares de seguridad IP son “obligatorios”, el IPSec debe ser activado de forma manual por parte del administrador.

- La segunda prueba evidencio que: la activación de IPSec AH e IPSec ESP, en un sistema operativo Windows XP SP2, es un proceso complejo, porque es necesario, conocer el funcionamiento de los diferentes métodos a ser utilizados para la autenticación de dispositivos (kerberos, preshare key) y los diferentes algoritmos de cifrado como: MD5, SHA1, DES y 3DES, para seleccionar el más adecuado de acuerdo a las características y necesidades especificas que posea la red a proteger, esta decisión la realiza el administrador de la red. De igual manera se puede concluir, que en un ambiente Windows, IPSec AH ofrece autenticación de extremo a extremo pero los datos viajan sin ser encriptados, por el contrario con IPSec ESP se hace tanto autenticación como encripción de datos.

- La cuarta prueba evidencio que: la activación de IPSec en un sistema operativo Linux Fedora Core 6, es un proceso sencillo comparado al proceso sobre Windows, porque sobre Linux, el administrador esta limitado a implementar sólo IPSec ESP e IPSec AH al mismo tiempo y no por separado, además, el intercambio de las llaves para la autenticación la hace de forma automática el protocolo IKA (racoon) de Linux, esto le evita al administrador el tener que seleccionar entre una lista de métodos para autenticación o cifrado.

Como conclusión final cabe recalcar que sobre el estándar IPv6, activar manualmente los protocolos de seguridad en un ambiente Windows XP SP2, no

tuvo efecto alguno, porque ni la autenticación ni la encripción se realizaron de la misma manera tal como sucedió con IPv4, por tal razón se recomienda o bien utilizar un sistema operativo diferente como por ejemplo Linux o implementar la seguridad a nivel de routers con el uso de VPNs.

7. TRABAJOS FUTUROS

Como trabajos futuros basados en seguridad IP, estarían la realización de un estudio que permita un análisis comparativo de la robustez y capacidades de los protocolos IPSec AH y ESP. Ya que la seguridad debe ser aplicada finalmente por el usuario o administrador de la red, esto hace posible configurar y definir diferentes parámetros a los encabezados de IPSec, tales como diferentes métodos de autenticación (kerberos, preshare key) y algoritmos de cifrado (SHA1, DES, 3DES), debido a esta situación seria conveniente, el realizar un estudio que consigne las capacidades y vulnerabilidades de cada opción lo que le permitirá al usuario seleccionar el mas adecuado, de acuerdo a sus capacidades y a las necesidades especificas de la red.

BIBLIOGRAFÍA

BENOIT Lourdelet, Cisco System All rights reserved. Cisco IOS NAT-PT for IPv6. [En línea]. 2003. [Citada el 18 de agosto Del 2006]. Disponible en Internet en: <http://www.cisco.com/application/pdf/en/us/guest/tech/tk361/c1550>.

Capas del modelo TCP/IP. TCP/IP Unleashed, Timothy Parker, Ph.D., et al. SAMS publishing. Copyright 1996 by Sams publishings. p. 27.

CAMARGO, Edwin. Tesis sobre plan de transición del protocolo de IPv4 a IPv6 en la Universidad Industrial de Santander. [En línea]. Bucaramanga 2006. [Citada el 18 de agostos de 2007]. Disponible en Internet en: <http://www.uis.edu.co>

CISCO, Products Configuration Guide. [En línea]. 2007. [Citado en Marzo 10 del 2007]. Disponible en Internet en: <http://www.cisco.com/en/US/products/ >

Cisco System. Cisco System Inc. All rights reserved. Cisco Feature Navigator. [En línea]. 1992. [Citada el 11 de agosto del 2006]. Disponible en Internet en: <http://www.cisco.com/ >.

HINDEN, R. Cisco Systems All rights reserved. IP Versión 6 Addressing Architecture. [En línea]. 1998. [Citada el 18 de agosto del 2006]. Disponible en Internet en: < http://www.ietf.org/rfc/rfc2373.txt>

How IPv6 Works, Microsoft Corporation. All rights reserved. Encapsulado y desencapsulado de un paquete IPv6. [En línea]. 2006. [Citado el 18 de agosto del 2007]. Disponible en Internet en: <http://technet2.microsoft.com/WindowsServer/en/library>.

IPv6 Project Status. Ivette Reategui. Diferencias entra IPv4 e IPv6. [En línea]. 2002. [Citado el 18 de agosto del 2006]. Disponible en Internet en: <http://www.rds.yahoo.com/>

KENT, S. BBN Technologies All rights reserved. IP Authentication Header RFC 4302. [En línea]. 2005. [Citada el 16 de agosto del 2006]. Disponible en Internet en: <ftp://ftp.rfc-editor.org/in-notes/rfc4302.txt>.

Microsoft techNet, Microsoft Corporation. All rights reserved. Transport Mode. [En línea]. 2006. [Citada el 16 de agosto del 2007]. Disponible en Internet en: <http://www.technet2.microsoft.com/>.

Microsoft techNet. Microsoft Corporation. All rights reserved. Transport Mode. [En línea]. 2006. [Citada el 16 de agosto del 2007]. Disponible en Internet en: <http://www.technet2.microsoft.com/windowsserver/en/library/ >.

Modelo OSI. Cisco Certified Network Associated, Second edition, Todd Lammle, SYBEX. Copyright 2000 Sybex Inc. p. 5.

Networking and Access Technologies. Microsoft Corporation. All rights reserved. Estructura de una dirección IPv4 clase A. [En línea]. 2006. [Citada el 28 de agosto del 2007]. Disponible en Internet en: <http://www.technet.microsoft.com/en-us/library/bb726995.aspx >.

NORDMARK, E. Sun Microsystems All rights reserved. Basic Transition Mechanisms for IPv6 Hosts and Routers. [En línea]. 2005. [Citada el 11 de agosto Del 2006]. Disponible en Internet en: < http://www.ietf.org/rfc/rfc4213.txt >

OIF OPTICAL INTERNETWORKING FORUM. [En línea]. 2003. [Citada el 18 de Enero de 2007]. Disponible en Internet en: <http://rds.yahoo.com>

Plan de transición del protocolo de IPV4 a IPv6 en la Universidad Industrial de Santander, [Citada el 18 de agosto del 2006].

SANTANA, Darwin. All rights reserved. IPv6: Plan de transición del protocolo de red ipv4 a ipv6. [En línea]. 2006 Santo Domingo [Citada el 18 de agosto del 2007]. Disponible en Internet en: <http://www.uis.edu.co >.

Technet. Microsoft Corporation All rights reserved. Introducing IPSec. [En línea]. 2006. [Citada el 14 de agosto del 2007]. Disponible en Internet en: <http://www.microsoft.com >.