UNIVERSIDAD POLITECNICA SALESIANA

FACULTAD DE INGENIERIAS

SEDE QUITO - CAMPUS SUR

CARRERA DE INGENIERIA EN SISTEMAS

MENCION TELEMATICA

"ANALISIS DE LAS FUNCIONALIDADES DE LOS PROTOCOLOS DE SEGURIDAD IPSEC, IKE, ISAKMP SOBRE IPv6 E IMPLEMENTACION EN UNA RED PROTOTIPO BAJO INFRAESTRUCTURA CISCO"

TESIS PREVIA PARA LA OBTENCION DEL TITULO DE INGENIERA DE SISTEMAS

VASQUEZ CLAVIJO, JENNY ELIZABETH

DIRECTOR: Ing. JORGE LOPEZ

QUITO, ABRIL 2011

DECLARACION

Yo Jenny Elizabeth Vásquez Clavijo, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual; por su reglamento y por la normatividad institucional vigente.

Jenny Elizabeth Vásquez Clavijo

CERTIFICACION

Certifico que el presente trabajo fue desarrollado por la Srta. **JENNY ELIZABETH VASQUEZ CLAVIJO** bajo mi dirección.

Ing. Jorge López

AGRADECIMIENTO

En los pasos de mis años de estudios me he dado cuenta que hay un Inicio y un Final y por esta razón doy Gracias a Dios por darme la perseverancia y la lucha constante de todos los días por haber llegado a una de mis metas propuestas.

Un agradecimiento especial a mis Padres LUIS y SUSANA por darme el apoyo firme y moral en el trayecto de mi vida estudiantil, a mis hermanos EDWIN y MARIA EUGENIA por la comprensión la ayuda que me brindan todos los días.

A la Universidad que me permitió formarme Profesionalmente con la ayuda de mis maestros por transmitirme sus conocimientos durante mi carrera estudiantil y principalmente agradeciendo al Ingeniero JORGE LOPEZ que tuvo paciencia y confianza de guiarme en este proyecto.

JENNY VASQUEZ

DEDICATORIA

La presente tesis la dedico a mis PADRES y HERMANOS que gracias a sus consejos y palabras de aliento me saben guiar en mi vida para poder llegar a cumplir mis metas propuestas y la persona que me brindo los conocimientos y la ayuda constante para poder culminar este proyecto al Ingeniero JORGE LOPEZ por haber depositado la confianza en mí.

JENNY VASQUEZ

INDICE

CAPITULO I

1. Introducción……..... 16
1.1. Antecedentes…….. 19
1.2. Justificación…… 24
1.3. Objetivos…….. 30
1.3.1. Objetivo General…… 30
1.3.2. Objetivos Específicos…… 30

CAPITULO II

2. ESTUDIO DE LOS PROTOCOLOS DE SEGURIDAD DE IPV4 e IPV6..... 31
2.1. Evolución de Internet…… 32
2.1.1. Internet en la Sociedad…….. 35
2.2. Desarrollo de Internet a base de los protocolos TCP/IP……... 36
2.2.1. Estudio de las capas de la arquitectura TCP/IP…… 40
2.3. Análisis del Protocolo IPV4……... 44
2.3.1. Arquitectura del Protocolo IPv4…… 47
2.4. Seguridad del Protocolo TCP e IPV4…….. 50
2.4.1. Seguridad en Internet bajo IPv4…….. 52
2.4.2. Seguridad en las Capas…… 53
2.5. Análisis del Protocolo IPV6……... 55
2.5.1. Arquitectura del Protocolo IPv6…… 60
2.5.2. Cabecera del Protocolo IPv6…… 62
2.5.3. Direccionamiento de IPv6…….. 66
2.5.4. Seguridades del Protocolo IPv6…… 75

CAPITULO III

3. ESTRUCTURA DEL PROTOCOLO DE SEGURIDAD IPSec en IPv6…… 77
3.1. Introducción IPSec…… 78
3.1.1. Modo de Funcionamiento de IPsec…….. 80
3.2. Componentes de IPSec…… 82
3.2.1. Security Association (SA)…….. 82
3.2.1.1. Definición de SA…… 83
3.2.1.2. Modo de Operación SA……... 86
3.2.1.3. Combinación de SA……... 87
3.2.1.4. Base de Datos SA……... 90
3.2.1.4.1. Base de datos de Políticas de Seguridad (SPD)…… 91
3.2.1.4.2. Base de datos de Asociación de Seguridad (SAD)…… 92
3.2.1.5. Gestión de Claves de SA…… 94
3.2.1.6. Procesamiento de ICMP……..… 96
3.2.1.7. Procesamiento de MTU……..…… 99
3.2.2. Cabecera de Autentificación (AH)……... 100
3.2.2.1. Funcionamiento de la Cabecera de Autentificación……... 101
3.2.2.2. Estructura de la Cabecera de Autentificación……..… 103
3.2.2.3. Localización de la Cabecera de Autentificación……..… 105

3.2.2.4. Algoritmo de Autentificación……..…….. 108
3.2.3. Cabecera de Seguridad Encapsulada (ESP)…….…… 110
3.2.3.1. Funcionamiento ESP……. 111
3.2.3.2. Estructura del ESP……..…. 113
3.2.3.3. Localización de ESP…… 114
3.2.3.4. Algoritmo de Encriptación y Autentificación……..… 116
3.2.4. Criptografía…….. 117
3.2.4.1. Criptografía Simétrica o Privada…… 119
3.2.4.1.1. Cifrado en Bloques…….. 120
3.2.4.1.1.1. Algoritmo Criptográfico por Bloques……. 124
3.2.4.1.2. Cifrado en Flujo…… 125
3.2.4.1.2.1. Algoritmo Criptográfico por Flujo……..… 125
3.2.4.2. Criptografía Asimétrica o Publica……..…. 126
3.2.4.2.1. Algoritmos Asimétricos…… 127
3.2.4.3. Funciones del Hash……..…. 129
3.3. Protocolo IKE……. 130
3.3.1. Funcionamiento del protocolo IKE……... 131
3.3.2. Arquitectura del protocolo IKE……. 133
3.3.3. Intercambio de Claves……... 135
3.4. Protocolo ISAKMP……..…. 138
3.4.1. Funcionamiento del Protocolo ISAKMP…….. 139
3.4.2. Arquitectura del Protocolo ISAKMP……. 141
3.4.2.1. Cabecera de Carga Genérica del Protocolo ISAKMP……..... 143
3.4.3. Intercambio de Claves de ISAKMP…….. 145
3.5. Listas de Acceso (ACL)……. 150
3.5.1. Tipos de Listas de Acceso……. 152

CAPITULO IV

4. IMPLEMENTACION Y PRUEBAS DE LOS PROTOCOLOS DE SEGURIDAD PARA IPV6……. 155
4.1. Diseño Físico Implementado……... 155
4.2. Diseño Lógico Implementado……... 156
4.3. Requerimientos para la Red……. 157
4.3.1. Requerimientos de Hardware……... 157
4.3.1.1. Características del Router 2801…….. 157
4.3.2. Requerimientos de Software……. 159
4.4. Configuraciones de los Equipos……..…. 160
4.4.1. Instalación de IPv6 en la plataforma Windows XP……..... 160
4.4.2. Ingreso de la Dirección IPv6 en el Host…….. 164
4.4.3. Conexión al Router con Dirección IPv6……... 167
4.4.4. Configuración de las Interfaces y Protocolos del Router…… 172
4.4.4.1. Configuración de las Interfaces……..…. 172
4.4.4.1.1. Interface Fast Ethernet…… 173
4.4.4.1.2. Interface Serial…… 175
4.4.5. Implementación de Rutas Estáticas……..…. 177
4.4.6. Políticas de Negociación del Protocolo IKE……... 179
4.4.6.1. Fase I……..…. 179
4.4.6.1.1. Implementación del Protocolo ISAKMP…… 180

4.4.6.2. Fase II……..…... 183
4.4.6.2.1. Implementación del Protocolo IPSec…… 183
4.4.7. Implementación de Listas de Acceso…….. 186
4.4.8. Implementación del Túnel para el tráfico IPv6……... 190
4.5. Verificación de Conectividad de los Hosts A y B……... 192

CAPITULO V

5. Conclusiones y Recomendaciones…….. 195

5.1. Conclusiones……..…… 195
5.2. Recomendaciones……..…… 196

Bibliografía……... 197
Anexos…….. 200

INDICE DE FIGURAS

FIG 2.1-1 Primer Diseño TCP/IP…… 34
FIG. 2.1-2 Estructura Jerárquica…… 34
FIG. 2.2-3 Modelo OSI con ISO vs TCP/IP…… 38
FIG. 2.2-4 Capas de TCP/IP…… 40
FIG. 2.3-5 Formato de las direcciones IPv4…… 44
FIG. 2.3-6 Subdivisión de los 32 bits para las clases A, B, C, D, E…… 46
FIG. 2.3-7 Estructura de un Datagrama IPv4…… 47
FIG. 2.4-8 Ubicación de los Protocolos en las capas superiores…… 53
FIG. 2.5-9 Estructura de un Datagrama IPv6…… 60
FIG. 2.5-10 Cabecera de Encaminamiento…… 63
FIG. 2.5-11 Cabecera de Fragmentación de datagramas…… 63
FIG. 2.5-12 Cabecera de opciones de destino…… 64
FIG. 2.5-13 Cabecera de autentificación IPv6…… 65
FIG. 2.5-14 Direccionamiento Unicast IPv6…… 66
FIG. 2.5-15 Direccionamiento Multicast IPv6…… 69
FIG. 2.5-16 Direccionamiento Anycast IPv6…… 71
FIG. 3.1-17 Arquitectura IPSEC…… 79
FIG. 3.1-18 Modo Transporte de IPSec…… 81
FIG. 3.1-19 Modo Túnel de IPSec…… 82
FIG. 3.2-20 Modo Transporte SA…… 85
FIG. 3.2-21 Modo Túnel SA…… 86
FIG. 3.2-22 Combinación básica de SA (caso 1)…… 88
FIG. 3.2-23 Combinación básica de SA (caso 2)…… 89
FIG. 3.2-24 Combinación básica de SA (caso 3)…… 89
FIG. 3.2-25 Combinación básica de SA (caso 4)…… 90
FIG. 3.2-26 Funcionamiento de la Cabecera de Autentificación…… 102
FIG. 3.2-27 Estructura de la Cabecera de Autentificación…… 104
FIG. 3.2-28 Modo Transporte de AH…… 107
FIG. 3.2-29 Modo Túnel de AH…… 108
FIG. 3.2-30 Funcionamiento de ESP…… 112
FIG. 3.2-31 Estructura de ESP…… 113
FIG. 3.2-32 Modo Transporte de ESP…… 115
FIG. 3.2-33 Modo Túnel de ESP…… 116
FIG. 3.2-34 Criptografía de Sistema Simétrico…… 120
FIG. 3.2-35 Funcionamiento del modo ECB…… 122
FIG. 3.2-36 Funcionamiento del modo CBC…… 123
FIG. 3.2-37 Funcionamiento del modo CFB…… 124
FIG. 3.3-38 Funcionamiento del Protocolo IKE…… 132
FIG. 3.3-39 Modo Principal del Protocolo IKE…… 136
FIG. 3.3-40 Modo Agresivo del Protocolo IKE …… 137
FIG. 3.3-41 Modo Rápido del Protocolo IKE …… 138
FIG. 3.4-42 Formato de la Cabecera ISAKMP…… 141
FIG. 3.4-43 Formato de la Cabecera de Carga Genérica…… 143
FIG. 4.1-44 Diseño Físico Implementado en Cisco …… 155
FIG. 4.2-45 Diseño Lógico Implementado en Cisco …… 156

FIG. 4.4-46 Conexión de Red……. 161
FIG. 4.4-47 Propiedades de la Conexión de Red…….. 161
FIG. 4.4-48 Tipo de Componente de Red…… 162
FIG. 4.4-49 Protocolo de Red…… 162
FIG. 4.4-50 Instalación de IPv6…….. 163
FIG. 4.4-51 Ingreso a modo Consola…… 163
FIG. 4.4-52 Instalación de IPv6 por Consola…….. 164
FIG. 4.4-53 Tipo de Interfaz que trabaja el Host……. 166
FIG. 4.4-54 Dirección loopback IPv6……. 166
FIG. 4.4-55 Dirección IPv6……. 167
FIG. 4.4-56 Ingreso a Modo Consola…… 168
FIG. 4.4-57 Información de Conexión…….. 169
FIG. 4.4-58 Descripción de la Conexión……. 169
FIG. 4.4-59 Selección del Puerto para la Comunicación…… 170
FIG. 4.4-60 Configuración del Puerto COM1……... 170
FIG. 4.4-61 Router esta encendido…….. 171
FIG. 4.4-62 Comandos de la Interface FAS 0/1 (Router 1, 2)……... 174
FIG. 4.4-63 Comandos de la Interface Serial 0/3/0 (Router1, 2)…… 176
FIG. 4.4-64 Implementación de Rutas Estáticas (Router 1, 2)…….. 178
FIG. 4.4-65 Implementación de la Política IKE en Fase I (Router 1, 2)……... 182
FIG. 4.4-66 Implementación de la Política IKE en Fase II (Router 1, 2)…….. 186
FIG. 4.4-67 Implementación de Listas de Acceso (Router 1, 2)……... 189
FIG. 4.4-68 Implementación del Túnel (Router 1, 2)…….. 192
FIG. 4.4-69 Verificación de Conectividad entre Hosts…… 193
FIG. 4.4-70 Verificación de paquetes Encriptados…….. 194

INDICE DE TABLAS

Tabla. 2.2-1 Como Trabaja TCP/IP……. 39
Tabla. 2.3-2 Clases de direcciones IP en Internet…… 46
Tabla. 2.5-3 IPv4 vs IPv6……..... 56
Tabla. 2.5-4 Prefijos reservados de la dirección Unicast global…….. 68
Tabla. 2.5-5 Significados de los bit de ámbito…….. 70
Tabla. 2.5-6 Tipo de Direccionamiento IPv6……. 73
Tabla. 3.2-7 Relleno de los bytes en el algoritmo de cifrado por bloques..... 121
Tabla. 3.3-8 Notación y significados para la Arquitectura del Protocolo IKE…….. 133
Tabla. 3.4-9 Notación y significados para el Intercambio de Claves de ISAKMP.. 145
Tabla. 3.5-10 Listas de Acceso disponibles……. 152
Tabla. 4.3-11 Requerimientos de Hardware de la Red…….. 157
Tabla. 4.3-12 Características Generales del Router 2801……. 159
Tabla. 4.3-13 Requerimientos del Software de la Red……... 160
Tabla. 4.4-14 Requisitos de Configuración……..... 172
Tabla 4.4-15 Fase 1 del protocolo IKE……. 179
Tabla 4.4-16 Fase 2 del protocolo IKE……. 183

RESUMEN

El presente proyecto de Grado titulado: Análisis de las funcionalidades de los Protocolos de Seguridad IPSec, IKE, ISAKMP sobre IPv6 e Implementación en una Red Prototipo bajo Infraestructura Cisco, radica en el análisis de las seguridades de las comunicaciones, como las funcionalidades y ventajas que se utilizan es los protocolos IPSec, IKE, ISAKMP cuando la información viaja desde el Emisor hasta el Receptor de acuerdo a la investigación realizada.

La gran demanda de usuarios en Internet ha producido que las direcciones existentes en IPv4 estén llegando al agotamiento como colapsando las tablas de encaminamiento de los Routers. Este protocolo presenta ciertas limitaciones en la actualidad y requiere de mecanismos de seguridad en la capa de red ya que esta no es segura, debido a estas desventajas se creó IPv6.

IPv6 se convertirá en el gran sucesor de las redes que ayudara a dar seguridad e integridad de los datos, también se solucionará las limitaciones de IPv4 en las redes permitiendo tener mayor espacio de direcciones de 128 bits y podrá tener una buena calidad de servicios, movilidad, velocidad en los datos. Como solución a los problemas de seguridad aparece el protocolo Seguridad IP (IPSec) que es utilizado de forma obligatoria, se basa en la criptografía moderna que garantiza la privacidad y la autentificación fuerte de datos, su característica lo hace único debido a que implementa seguridad en la capa de red, garantiza que las aplicaciones que se estén usando en la red sean seguras. IPsec se puede implementar en modo transporte que permite la comunicación de host a host y también se puede usar en modo túnel que se utiliza para comunicaciones de: red a red, host a red o host a host por medio de Internet.

Se debe tener en cuenta que el componente que se desarrollan dentro de IPsec es la Asociación de Seguridad (SA) que consiste en una conexión unidireccional simplex que define las medidas de seguridad que se deben aplicar a paquetes basados en: Quién los manda, a dónde van y el tipo de datos que viaja por la red y puede ser utilizado en forma de modo transporte o túnel.

Cada nodo IPsec debe mantener dos bases de datos: La Base de Datos de Políticas de Seguridad que contiene las políticas definidas por el administrador según las necesidades de seguridad del tráfico IP que entra y sale del nodo. Y la Base de datos de Asociación de Seguridad que define los parámetros de todas las asociaciones de seguridad activas.

Para la implementación de IPsec se debe utilizar de forma obligatoria algoritmos de Encriptación que es usado por la cabecera de Seguridad Encapsulada (ESP) y el Algoritmo de Autentificación es usado para la comunicación punto a punto y los más aptos son DES, 3DES o funciones del hash unidireccionales como MD5 o SHA-1. En el capítulo 3 se detallará cada algoritmo y las funcionalidades que contiene cada criptografía dentro la SA con los protocolos IKE, ISAKMP.

Las funcionalidades de IPSec, son los mecanismos principales para el funcionamiento de las seguridades en las comunicaciones los cuales son: La Cabecera de Autentificación que se usa para proporcionar integridad sin conexión, autentificación del origen de los datos, dar protección contra reenvíos y verificar que los datos no sean alterados cuando la información viaje de extremo a extremo. El siguiente mecanismo es la Cabecera de Seguridad Encapsulada que provee confidencialidad de tráfico IP y seguridad que puede ser aplicado solo o en conjunto con la cabecera de autentificación también en forma anidada como es el modo túnel.

Dentro de estas funcionalidades se encuentra el protocolo de Gestión de Claves y Asociación de Seguridad en Internet (ISAKMP) es el escogido para el intercambio de claves y parámetros de seguridad en IPSec, utiliza el concepto de seguridad necesario para el establecimiento de SA y claves criptográficas en un entorno de Internet.

El protocolo de Intercambio de Claves de Internet (IKE) resuelve el problema más importante del establecimiento de comunicaciones seguras, su propósito es negociar y proveer material de claves autenticado para las Asociaciones de Seguridad de una manera protegida. Este tipo de protocolo funciona en dos fases: La Primera fase se define las seguridades a través de la Autentificación y Encriptación que genera el Protocolo ISAKMP como el algoritmo de cifrado por

bloques, algoritmo hash, método de autentificación, el intercambio de claves y en la Segunda fase se realiza el intercambio de propuestas de asociaciones de Seguridad y negocia las asociaciones basándose en el ISAKMP, también se definen las seguridades a través de IPsec que ofrece en modo transporte o modo túnel.

Para que los protocolos de seguridad IPSec, IKE, ISAKMP funcionen correctamente y el tráfico que viaje por la red sea activado por el túnel se debe crear Listas de Acceso porque se necesita filtrar el tráfico que entra y sale de la red de esta manera la información viajara por el túnel y se aplicara políticas de seguridad que permita o niega el acceso de cierta parte de la red a otra de acuerdo a alguna condición.

La investigación realizada permite conocer que los paquetes que viajen por el túnel desde el Emisor hasta el Receptor llegarán encriptados o encapsulados de esta forma se concluye que los protocolos de seguridad mencionados anteriormente son esenciales como las listas de acceso que permitirán que el tráfico sea activado y de esta forma se podrán verificar que los paquetes llegan de forma segura.

PRESENTACION

Este proyecto está estructurado en 5 Capítulos, los cuales están detallados de la siguiente manera:

CAPITULO I

El Capítulo I contiene la introducción, antecedentes, justificación y objetivos de lo que se ha realizado en este proyecto y adicionalmente se da una introducción a los protocolos de seguridad que se han usado.

CAPITULO II

El Capítulo II se hace un estudio de los protocolos de seguridad de IPv4 e IPv6 y se da a conocer como evolucionó Internet en el campo de las comunicaciones hasta la actualidad.

CAPITULO III

El Capítulo III se realiza un análisis de la estructura del protocolo de seguridad IPSec en IPv6, con el respectivo funcionamiento y los componentes que se utilizan para dar la seguridad a las comunicaciones a través de los protocolos IKE, ISAKMP y a demás se detalla el uso de Listas de Acceso para qué el tráfico pueda ser activado en el túnel de esta manera la información pueda llegar encriptada.

CAPITULO IV

El Capítulo IV muestra la Implementación de la Red Prototipo y las pruebas de los protocolos de seguridad para IPv6, demostrando el diseño físico y lógico implementado en la red con las configuraciones realizadas en los equipos.

CAPITULO V

El Capitulo V se expone las conclusiones y recomendaciones obtenidas del proyecto realizado.

CAPITULO I

1. INTRODUCCION

Internet es la red de computadoras más grandes de todo el mundo, de la que forman parte miles de redes que se encuentran distribuidas en todo el planeta. Su origen tuvo lugar en los años 60, con una red exclusivamente militar llamada ARPANET, desarrollada por Advanced Research Projects Agency del Departamento de Defensa de los Estados Unidos.

En un principio la conexión entre computadoras sólo era posible entre modelos de una misma marca, llegándose incluso a dar el caso de que diferentes modelos de un mismo fabricante no podían comunicarse entre sí. La conexión sólo era posible entre dos computadoras (vía línea telefónica, comunicación por un puerto serie o paralelo). Tanto fue el crecimiento de la red que su sistema de comunicación se quedo obsoleto.

A partir de los años 70, las redes de interconexión de computadoras ya habían avanzado bastante, permitiendo la comunicación de diferentes tipos de máquinas. Para conseguir este objetivo, fue básico que organismos internacionales como IEEE[1], ISO[2] regularan los mecanismos y formas en que se debían realizar las comunicaciones entre equipos informáticos. Se definió un modelo teórico denominado modelo OSI[3], que especificaba un conjunto de 7 capas que permiten aislar el computador de la red a la que se encontraba conectado, permitiendo la interconexión de diferentes computadoras a una misma red.

Una vez conseguida la conexión de máquinas diferentes en una misma red, se pasó a una segunda fase que consistió en la comunicación entre los diferentes tipos de redes existentes hasta formar la gran red de redes que actualmente se denomina **INTERNET**.

---

[1] **IEEE:** Institute of Electrical and Electronics Engineers: Importante asociación de técnicos y profesionales destinados a la investigación de las computadoras, comunicaciones.

[2] **ISO**: Organización Internacional para la Estandarización. Es una organización que ha definido un conjunto de protocolos diferentes, llamados protocolos ISO/OSI

[3] **OSI:** Interconexión de Sistemas Abiertos. Es el protocolo en el que se apoya Internet

De esta forma se desarrolló una nueva tecnología conocida como Packet Switching (conmutación de paquetes) que recibió el nombre de Transmission Control Protocol e Internet Protocolo (TCP/IP)

INTERNET utiliza esta familia de protocolos TCP/IP (entre los que se pueden destacar TCP, UDP e IP). **IP** (Internet Protocol) es un protocolo de interconexión de redes heterogéneas que se encarga del transporte de los datagramas (paquetes de datos) a través de la red**. UDP** (User Datagram Protocol) es un protocolo de comunicación entre computadoras de nivel superior al IP, sin conexión y que no proporciona fiabilidad a la comunicación. **TCP** (Transmission Control Protocol) es también un protocolo de nivel superior al IP, pero orientado a la conexión y fiabilidad.

Actualmente la red de redes Internet está regida por la versión 4 del protocolo IP que recibe el nombre de IPv4. Sin duda alguna ha proporcionado los medios para que Internet haya podido evolucionar desde una red que conectaba apenas unos pocos centros de investigación a mediados de los 80 hasta convertirse en la Red de redes que todos conocen hoy en día. Gracias a IPv4, Internet se ha convertido en uno de los motores actuales de la sociedad no solo en el campo tecnológico y económico sino también en aspectos sociales.

Sin embargo debido al ritmo de crecimiento tan fuerte e inesperado de Internet, IPv4 está llegando a su extinción. En 1992, la IANA[4] (Internet Assigned Numbers Authority) predijo que el aumento de usuarios en los últimos años, produciría el agotamiento del espacio de direccionamiento de IPv4 por lo que se constituyó un grupo de trabajo en el IETF[5] llamado IPng (IP Next Generation) con la intención de desarrollar un nuevo protocolo de Internet que fuera el sucesor de IPv4.

Fruto de los trabajos de IETF a mediados de los 90 se propuso el protocolo que está llamado a ser el sucesor denominado IPv6

---

[4] **IANA:** Internet Assigned Numbers Authority: delega la asignación de dominios para la administración de direcciones IP

[5] **IETF**: Internet Engineering Task Force: es una organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet

Esta versión del protocolo IP es la número 6, que por cuestiones de nomenclatura ha pasado a denominarse IPv6 (IP versión 6) o IPng (IP next generation).

Esta revisión de las especificaciones actuales del protocolo IP ha sido motivada principalmente al hecho de que el sistema de direccionamiento actualmente se utilizan 32 bits, se ha quedado pequeño debido al gran auge de Internet (en los últimos 10 años se ha experimentado un crecimiento superior al 600%), y no se puede absorber la demanda de nuevas direcciones.

Además, los últimos servicios que se ofrecen sobre esta red (comercio electrónico o e-comerce, redes corporativas o Virtual Private Networks, video-conferencia) requieren de componentes tanto de velocidad como de seguridad y autenticidad que la versión 4 del protocolo IP no contempla. Todo esto ha provocado la creación de algunas extensiones de seguridad.

IPv4 no define una seguridad de información entre diferentes usuarios por el cual se crea un mecanismo dominante escalable y seguro para la distribución de llaves ISAKMP, IKE para asegurar la información entre varios usuarios.

La tecnología en la actualidad ofrece seguridades en los mensajes entre el emisor y receptor creando protocolos de seguridad mediante IPv6. Estos protocolos permitirán que los mensajes que se envíen al receptor, viajen de forma encriptada a través de las políticas IKE, ISAKMP e IPSec.

IPSec (IP Security) proporciona servicios de seguridad en la capa IP, permitiendo a un sistema seleccionar los protocolos de seguridad para proporcionar los servicios solicitados por los usuarios. En el capítulo 3 se detalla la funcionalidad del protocolo IKE, ISAKMP e IPSec.

1.1 ANTECEDENTES

La creación de un sistema de comunicación produjo un gran auge y se dio la necesidad de expandir sus rutas para poder enviar y transmitir información. Los que idearon y pusieron en funcionamiento este tipo de comunicación no evaluaron la gran trascendencia que tiene hasta la actualidad.

Internet va evolucionando constantemente por lo cual se debe tener en cuenta las seguridades, que es un punto importante y algunos de los protocolos implementados no son seguros.

Esta red comenzó utilizando el concepto de comunicación por paquetes de datos para transmitir la información, y estaría compuesta de nodos de características similares que tendrían la capacidad de recibir, pasar y originar paquetes.

La idea principal de la red es que no hay una ruta establecida que deban de recorrer los paquetes desde su origen hasta su destino. El paquete es pasado de un nodo a otro, orientado de modo general hacia su destino, hasta que llega al receptor correcto. Estos nodos eran llamados supercomputadoras.

Poco a poco la red fue creciendo debido a su estructura descentralizada y siempre y cuando las computadoras que ampliaban la red utilizaran el protocolo de comunicación adecuado.

El protocolo original de comunicación que fue utilizado por las computadoras de la red fue el NCP[6] (Network Control Protocol), pero fue después reemplazado por el protocolo TCP/IP mucho más avanzado.

El protocolo IP es parte de la capa de Internet del conjunto de protocolos TCP/IP. Es uno de los protocolos de Internet más importantes ya que permite el desarrollo y transporte de datagramas de IP (paquetes de datos), aunque sin garantizar su entrega. En realidad, el protocolo IP procesa datagramas de IP de manera independiente al definir su representación de ruta y envío.

---

[6] **NCP:** Network Control Protocol. Conjunto original de Protocolo de Control de Red de ARPANET

Las direcciones IP que se envían al destinario están formados por 3 campos:

- El campo de dirección IP: Dirección del equipo
- El campo de máscara de subred: una máscara de subred le permite al protocolo IP establecer la parte de la dirección IP que se relaciona con la red.
- El campo de pasarela predeterminada: le permite al protocolo de Internet saber a qué equipo enviar un datagrama, si el equipo de destino no se encuentra en la red de área local.

Los datagramas son datos encapsulados, es decir, datos a los que se les agrega un encabezado que contiene información (como la dirección IP de destino).

De esta forma los routers analizan (y eventualmente modifican) los datos contenidos en un datagrama.

Los equipos se comunican a través de Internet mediante el protocolo IP utilizan direcciones numéricas denominadas direcciones IP que se implementa con un número de 32 bit que suele ser mostrado en cuatro grupos de números decimales de 8 bits.

Cada uno de esos números se mueve en un rango de 0 a 255 (expresado en decimal), o de 0 a FF (en hexadecimal) o de 0 a 11111111 (en binario). El valor decimal de cada octeto puede ser entre 0 y 255 (el número binario de 8 bits más alto es 11111111 y esos bits de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 256 en total, 255 más el 0 (0000 0000)).

El organismo a cargo de asignar direcciones IP para los equipos conectados directamente a la red pública de Internet, es el ICANN (Internet Corporation for Assigned Names and Numbers) que remplaza el IANA desde 1998.

IPv4 usa direcciones de 32 bits, limitándola a 2^{32} = 4.294.967.296 direcciones únicas, muchas de las cuales están dedicadas a redes locales (LANs) Por el crecimiento enorme que ha tenido Internet (mucho más de lo que esperaba, cuando se diseñó IPv4), combinado con el hecho de que hay desperdicio de direcciones y escases de las mismas.

Las direcciones IP se dividen en clases A, B, C de acuerdo a la cantidad de bytes que representan a la red.

El objetivo de dividir las direcciones IP en clases A, B, C es facilitar la búsqueda de un equipo en la red. De hecho, con esta notación es posible buscar primero la red a la que se desea tener acceso y luego buscar el equipo dentro de esta red. Por lo tanto, la asignación de una dirección de IP se realiza de acuerdo al tamaño de la red

Una dirección IP debe tener una máscara que permite distinguir los bits que identifican la red y los que identifican el host de una dirección IP, se genera con números 1 en la ubicación de los bits que se quiera conservar y 0 en aquellos que quiera cancelar los bits. Una vez que se crea una máscara, simplemente se coloca un Y lógico entre el valor que quiere enmascarar y las máscara, a fin de mantener intacta la parte deseada y cancelar el resto.

Por lo tanto una máscara de red se presenta bajo la forma de 4 bytes separados por puntos (como una dirección IP), y está compuesta (en su notación binaria) por ceros en lugar de los bits de la dirección IP que se desea cancelar (y por unos en lugar de aquellos que se quiera conservar).

En las direcciones IP se pueden originar máscaras de subredes, su interés principal reside en que permite la identificación de la red asociada con una dirección IP.

Efectivamente, la red está determinada por un número de bytes en la dirección IP (1 byte por las direcciones de clase A, 2 por las de clase B y 3 bytes para la clase C). Sin embargo, una red se escribe tomando el número de bytes que la caracterizan y completándolo después con ceros

El espacio de direcciones de una red puede ser subdividido a su vez creando subredes autónomas separadas

A medida del gran crecimiento de usuarios que se da año a año se dio la necesidad de implementar nuevas versiones de protocolos

IPv4 es la versión 4 del Protocolo IP. Esta fue la primera versión del protocolo que se implementó extensamente, y forma la base de Internet.

IPv4 tiene grandes limitaciones como:

- Número máximo de direcciones = 2^{32} = 4 mil 300 millones
- Redes de clase A: 15 millones nodos.
- Redes de clase B: 64000 nodos (más popular).
- Redes de clase C: 250 nodos (muy chica).

Este tema ha sido una preocupación desde los años 80s. Como consecuencia, se ha convertido en el factor impulsor en la creación y adopción de diversas nuevas tecnologías.

El desperdicio de direcciones IPv4 se debe a varios factores. Uno de los principales es inicialmente no se consideró el enorme crecimiento que iba a tener Internet; se asignaron bloques de direcciones grandes (de 16,271 millones de direcciones) a países, e incluso a empresas.

Otro motivo de desperdicio es en la mayoría de las redes, exceptuando las más pequeñas, resulta conveniente dividir la red en subredes. Dentro de cada subred, la primera y la última dirección no son utilizables; de todos modos no siempre se utilizan todas las direcciones restantes.

Esta limitación ayudó a estimular el impulso hacia IPv6, que está actualmente en las primeras fases de implantación, y se espera que termine reemplazando a IPv4.

El protocolo IPv6 es el encargado de dirigir y encaminar los paquetes en la red, fue diseñado en los años 70 con el objetivo de interconectar redes.

Usa direcciones de 128 bits $2^{128} = 3.4x10^{38} => 665x10^{21}$ direcciones por m^2 de la superficie de la tierra. Permite múltiples interfaces por host y múltiples direcciones por interface.

Quizás las principales características de la IPv6 se sintetizan en el mayor espacio de direccionamiento, seguridad, autoconfiguración y movilidad. Pero también hay otras que son importantes mencionar:

- Infraestructura de direcciones y enrutamiento eficaz y jerárquico.
- Mejora de compatibilidad para Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Movilidad: una de las características obligatorias de IPv6 es la posibilidad de conexión y desconexión de las computadoras en redes IPv6.

IPv6 proporcionará seguridad Integrada IPSec[7] que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello

[7] **IPSec:** Internet Protocol Security es un conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet

1.2 JUSTIFICACION

El presente proyecto se justifica a base de la gran demanda de usuarios en Internet debido al desarrollo de las redes de comunicaciones, tecnologías y servicios

La necesidad de mejorar las comunicaciones como su seguridad es debido al gran número de computadoras conectadas a INTERNET que utilizan TCP/IP.

Lo que implica que cualquier modificación de cualquiera de estos protocolos afecte a una gran variedad de computadoras y sistemas operativos.

Se debe plantear seriamente las necesidades actuales y futuras para asegurar que una revisión del protocolo es necesaria y aporte seguridad a los usuarios

Internet hoy en día está basado en un protocolo de red estandarizado que recibe el nombre de IPv4

IPv4 ha proporcionado los medios para que Internet haya podido evolucionar desde una red que conectaba apenas unos pocos centros de investigación a mediados de los 80 hasta convertirse en la Red de redes que todos conocen hoy en día.

Sin embargo debido al ritmo de crecimiento tan fuerte e inesperado de Internet, IPv4 está llegando a su extinción, debido al límite de direcciones con que fue creada, llegando al agotamiento el número de direcciones existentes como colapsando las tablas de encaminamiento de los Routers

Este protocolo presenta algunas limitaciones en la actualidad. Tiene inminente saturación del espacio de direcciones, también requiere mecanismo de seguridad en la capa de red ya que esta no es segura. Contiene escases de direccionamiento IP permitiendo una limitación del aumento de usuarios en internet

Como solución a las limitaciones de IPv4 aparece la nueva versión llamada IPng considerado también como IPv6 en el cual el espacio de direcciones es

prácticamente infinito utilizando 128 bits y una jerarquía de direcciones, permitiendo la seguridad e integridad de los datos.

Otro de los grandes problemas del crecimiento de Internet es la capacidad de almacenamiento necesaria en las pasarelas (routers) y el tráfico de gestión preciso para mantener sus tablas de encaminamiento. Existe un límite tecnológico al número de rutas que un nodo puede manejar, y como Internet crece de forma mucho más rápida que la tecnología que la mantiene, se intuye que pronto las pasarelas alcanzarán su capacidad máxima y empezarán a desechar rutas, con lo que la red comenzará a fragmentarse en subredes sin acceso entre sí.

La seguridad con la aparición de servicios comerciales y la conexión de numerosas empresas, el enorme incremento en el número de usuarios por todo el planeta y la cantidad de sistemas que necesitan de Internet para su correcto funcionamiento, es urgente definir mecanismos de seguridad para la red. Son necesarios esquemas de autenticación y privacidad, tanto para proteger a los usuarios en sí, como la misma integridad de la red ante ataques malintencionados o errores.

IPv4 define una red pura orientada a datagramas y, como tal, no existe el concepto de reserva de recursos. Cada datagrama debe competir con los demás y el tiempo de tránsito en la red es muy variable y sujeto a congestión. Por ello, se necesita una extensión que posibilite el envío de tráfico de tiempo real, y así poder hacer frente a las nuevas demandas en este campo.

IPv6 brinda más seguridad, la autenticación y confidencialidad constituyen las funciones de seguridad más importantes del protocolo versión 6

Todas las limitaciones que contiene IPv4 serán solucionados con la versión del protocolo IPv6. Esta nueva versión tiene grandes soluciones que son superiores y seguras.

Entre las ventajas que se dan entre IPv6 con respecto a IPv4 se puede mencionar las principales:

- Direcciones más largas.: El nuevo tamaño de la dirección es el cambio más notable. IPv6 cuadriplica el tamaño de la dirección del IPv4 de 32 a 128bits.

El espacio disponible para una dirección IPv6 es tan grande que no puede llegar a agotarse en un futuro previsible.

- Formatos de cabecera flexible: IPv6 utiliza un nuevo formato de datagrama. A diferencia del IPv4, que utiliza una cabecera de datagrama de formato fijo, donde todos los campos, excepto la parte opcional ocupan un número fijo de octetos, el IPv6 utiliza un conjunto opcional de cabeceras.

- Fragmentación end-to-end: Esta ventaja radica en el hecho de que a los enrutadores se les elimina la función de fragmentar los paquetes que les lleguen debido al MTU[8]. En cambio, esta función queda determinada para el nodo de origen que quiere enviar la información por medio de la red.

- Soporte para reserva de recursos: IPv6 reemplaza la especificación del tipo de recursos del IPv4 con un mecanismo que permite la reserva con anterioridad de recursos de red. En particular, el nuevo mecanismo soporta aplicaciones corno video en tiempo real, el cual requiere que se garantice el ancho de banda y el retardo.

- Número de saltos: Al cambiarse el tiempo de vida en un paquete IPv4 por el número de saltos en IPv6 se está mejorando el hecho de que si existe congestión en la red, este paquete no sea eliminado sin que tenga la opción de llegar hasta el nodo de destino. Como es bien sabido, en TCP el camino es establecido desde un principio, y por lo tanto se sabe de antemano cuál es el número de nodos por los que debe pasar.

Es evidente que son muchas las ventajas de IPv6 con respecto a IPv4 y es evidente que la autentificación y confidencialidad constituye las funciones de seguridad más importantes del protocolo IPv6

---

[8] **MTU:** La unidad máxima de transferencia. Redes de computadoras que expresa el tamaño en bytes de la unidad de datos más grande que puede enviarse usando un Protocolo de Internet

Uno de los objetivos del proceso de migración a IPv6 permite a los routers como los servidores compatibles con el nuevo protocolo sean introducidos en el mercado gradualmente lo que permitirá tanto al fabricante como a administradores de sistemas y usuarios finales realizar el paso a la nueva versión a su propio ritmo.

El formato de IPv6 es una evolución de IPv4 y no se ha realizado grandes cambios de contenido o estructura, simplemente se ha mejorado y optimizado, lo que permite que prácticamente no se necesite realizar ningún trabajo extra en la actualización al nuevo protocolo.

Uno de los cambios que se hizo en la estructura de IPv6 es la cabecera del paquete así como en el proceso de reenvío para hacer el procesamiento más simple y eficiente para poder describir con mas detalles las opciones del paquete. En concreto se determinan:

- El encabezado del paquete en IPv6 es más simple que el utilizado en IPv4, donde los campos raramente utilizados fueron movidos a opciones separadas; en efecto, aunque las direcciones en IPv6 son 4 veces más largas, el encabezado IPv6 (sin opciones) es solamente el doble de largo que el encabezado IPv4 (sin opciones).

- Los routers IPv6 no hacen fragmentación. Los nodos IPv6 requieren ya sea hacer descubrimiento de PMTU[9], realizar fragmentación extremo a extremo o enviar paquetes menores al MTU mínimo de IPv6 de 1280 bytes.

- El campo Tiempo de Vida de IPv4 se llama ahora Límite de Saltos (Hop Limit), reflejando el hecho de que ya no se espera que los routers computen el tiempo que el paquete ha pasado en la cola.

Así, IPv6 puede ser instalado como una actualización de software en los dispositivos de red, siendo totalmente compatible con el actual protocolo.

---

[9] **PMTU:** Es la tecnología en computadores de redes para determinar la máxima unidad de transferencia, determina el tamaño de la red entre dos IP

Durante el periodo de coexistencia de ambos protocolos, los equipos que no hayan sido actualizados todavía podrán seguir trabajando, identificando antes con qué protocolo se realiza la comunicación que recibe en cada momento. Es decir, cada dispositivo deberá leer la cabecera del paquete recibido, en la que un campo de cuatro bits le especificará si el protocolo utilizado es IPv4 o IPv6.

Los verdaderos motores de la transición, son los propios usuarios. Son los usuarios finales los que van a tener la necesidad de migrar a IPv6 porque van a ver que pueden realizar nuevas aplicaciones y servicios, más seguridad, mayor calidad de servicio.

Como solución a los problemas de seguridad aparece el protocolo IPSec, que es obligatoria y no opcional como sucede en IPv4, permitiendo implementar otros protocolos de seguridad IKE[10], ISAKMP[11] en IPv6 para que los datos puedan llegar de forma segura y confidencial.

IPSec ofrece servicios de seguridad en la capa de IP habilitando un sistema para seleccionar protocolos de seguridad necesarios, determinar algoritmos a utilizar en los servicios y colocar en cualquier lugar las llaves criptográficas requeridas para cumplir con los servicios solicitados. Se utilizan dos protocolos para proveer seguridad: uno para autentificación, diseñado para el encabezado del protocolo AH, y otro combinado para autentificación / encriptamiento diseñado para el formato del paquete en el protocolo ESP (Cabecera de Seguridad Encapsulada). Los servicios proporcionados son:

- Control de acceso
- Integridad sin conexión
- Autentificación de origen
- Confidencialidad (encriptamiento)

---

[10] **IKE:** El protocolo para Intercambio de Claves en Internet

[11] **ISAKMP**: Internet Security Association and Key Management Protocol. Un protocolo criptográfico que constituye la base del protocolo de intercambio de claves IKE

- Rechazo de paquetes retocados (como una forma de integridad secuencial parcial)
- Confidencialidad limitada por el flujo del Tráfico

IPSec es un protocolo que provee seguridad punto a punto en IPv4 e IPv6 (en IPv6 el soporte IPSec viene implementado por defecto). IPSec es un estándar que poco a poco se está aceptando en las distintas plataformas, en GNU/Linux.

Este protocolo implementa cifrado a nivel del protocolo IP, por lo que todos los protocolos por encima de IP se pueden utilizar con IPSec de forma transparente.

El protocolo IKE resuelve el problema más importante del establecimiento de comunicaciones seguras: la autenticación de los participantes y el intercambio de claves simétricas.

Tras ello, crea las asociaciones de seguridad y rellena la SAD (Base de Datos de Asociación de Seguridad). El protocolo IKE suele implementarse a través de servidores de espacio de usuario, y no suele implementarse en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación

Con el desarrollo del presente proyecto se estará aportando a la seguridad de la información en IPv6, la investigación será una base fundamental que contribuirá al fortalecimiento de la vinculación entre grupos de investigación y para futuras implementaciones prácticas.

1.3 OBJETIVOS

1.3.1 OBJETIVO GENERAL

Analizar las funcionalidades de los protocolos de seguridad IPSec, IKE, e ISAKMP sobre IPv6 y diseñar una red prototipo bajo la infraestructura de Cisco

1.3.2 OBJETIVOS ESPECIFICOS

- Estudiar las especificaciones de IPv6, sus nuevas características y aportaciones así como sus semejanzas y diferencias con IPv4

- Diseñar una red prototipo que trabaje con los protocolos de Seguridad en IPv6 demostrando la seguridad de la información mediante estos protocolos

- Analizar los resultados obtenidos con los protocolos de seguridad mediante la red prototipo, los mismos que puedan demostrar la seguridad que se genera en IPv6.

- Implementar los protocolos IPSEC, IKE, ISAKMP y realizar las diferentes pruebas para comprobar sus capacidades prácticas así como sus ventajas e inconvenientes respecto a IPv4

CAPITULO II

2. ESTUDIO DE LOS PROTOCOLOS DE SEGURIDAD DE IPv4 e IPv6

Con la evolución de Internet y el gran crecimiento que se dio desde su aparición, se ha dado grandes cambios para su estudio principalmente los protocolos IPv4 e IPv6. Cuando se inicio Internet con el objetivo de comunicarse de una computadora a otras computadoras para transmitir información, se definió que los protocolos eran necesarios e importantes para la seguridad de los datos que se envían y reciben de los diferentes usuarios

IPv4 fue la primera versión que se implemento extensamente y forma la base de Internet, debido a la gran cantidad de usuarios inesperados, fue teniendo limitaciones en el funcionamiento de las redes actuales como inminentemente saturación del espacio de direcciones, las seguridad en la capa de red y era necesario implementar una nueva versión que no lo sustituya, sino que se pueda adaptar.

Debido a la escasez de direcciones IP se limita el crecimiento de Internet, lo que obstaculiza a nuevos usuarios para su uso, ya que posteriormente IPv4 se convirtió en una red pública para investigación y educación.

Como solución a los problemas surgidos en IPv4, se creó IPv6 lo que se convertiría en un gran sucesor de las redes que ayudará a dar seguridad e integridad de los datos

Con la llegada de IPv6 se solucionará las limitaciones de IPv4 en las redes, permitiendo tener más direcciones IP, una buena calidad de servicio, movilidad, velocidad en los datos.

El estudio de los protocolos de Internet es de suma importancia, ya que de generación en generación han ido cambiando para que las redes sean más seguras, flexibles para la sociedad.

2.1 EVOLUCION DE INTERNET

Las mayores aportaciones tecnológicas de Internet se centran en la aparición de los navegadores, la simplicidad y la potencia de los protocolos utilizados como el lenguaje de programación en red, que han provocado la aparición de nuevos modelos de servicios.

Internet ha evolucionado en el mundo de las computadoras y las comunicaciones de una forma radical sin precedentes. La invención del telégrafo y posteriormente la del teléfono, radio, computadoras y redes de paquetes sentaron las bases para esta integración de capacidades que hasta este momento parecían utópicas. Además, Internet representa uno de los mayores ejemplos de los beneficios obtenidos mediante la investigación y el desarrollo en el campo de la información.

La actual red Internet es fruto de la evolución de una serie de redes de computadoras y técnicas de comunicación, desarrolladas durante los últimos años.

En 1957 algunos autores citan el lanzamiento del Satélite Sputnik como el desencadenante de estas investigaciones. En los años 60 y 70, se vivía una situación de guerra fría y la distribución geopolítica del planeta aparecía como dos grandes bloques. Cualquier desarrollo tecnológico de una de las partes era considerado por la otra como una amenaza o un reto

En 1962 se documentaron sobre la creación de una red global para la conexión de computadoras denominada red galáctica, donde todas las computadoras estarían conectadas entre sí, permitiendo el acceso rápido a cualquier tipo de información.

ARPA desarrolló una nueva tecnología denominada conmutación de paquetes, cuya principal característica reside en fragmentar la información, dividirla en porciones de una determinada longitud a las que se llama paquetes. Cada paquete lleva asociada una cabecera con datos referentes al destino, origen, códigos de comprobación, etc. Así, el paquete contiene información suficiente como para que se le vaya encaminando hacia su destino en los distintos nodos que atraviese.

En 1969 nace la primera red interconectada ARPANET desarrollada por ARPA (Advanced Research Proyect Agency) o Agencia de Proyectos de Investigación Avanzados, del Gobierno USA. Esta red se basada en la "conmutación de paquetes", técnica en la que el mensaje se subdivide en bloques o "paquetes", se les añade una cabecera con información sobre su origen y destino permitiendo, si fuera necesario, su transmisión independiente. Comienza a funcionar oficialmente en 1971.

ARPANET la primera red, se construyó simplemente para sobrevivir a ataques nucleares que sigue siendo muy popular. Sin embargo, este no fue el único motivo, fue diseñada para sobrevivir a fallos en la red, la verdadera razón para ello era que los nodos de conmutación eran poco fiables.

En 1972 se realizó la primera demostración pública de ARPANET, una nueva red de comunicaciones financiada por DARPA[12] que funcionaba de forma distribuida sobre la red telefónica conmutada. El éxito de ésta nueva arquitectura sirvió para que DARPA iniciara un programa de investigación sobre posibles técnicas para interconectar redes (orientadas al tráfico de paquetes) de distintas clases. Para este fin, desarrollaron nuevos protocolos de comunicaciones que permitiesen este intercambio de información de forma "transparente" para las computadoras conectadas. De la filosofía del proyecto surgió el nombre de "Internet", que se aplicó al sistema de redes interconectadas mediante los protocolos TCP e IP.

Para que las computadoras puedan comunicarse entre sí es necesario que todos ellos envíen y reciban la información de la misma manera. La descripción de los pasos a seguir se denomina “protocolo”.

Se presenta el concepto de arquitectura abierta sobre el que se fundamentará ARPANET. Esta versatilidad de no depender de ninguna computadora o red en concreto, permite la interconexión de nodos heterogéneos en una red homogénea.

---

[12] **DARPA: D**efense **A**dvanced **R**esearch **P**rojects **A**gency es una agencia del Departamento de Defensa de los Estados Unidos responsable del desarrollo de nuevas tecnologías para uso militar.

Después de algunas versiones de evaluación, se llegó a la conclusión de que el protocolo debería subdividirse en dos. Un protocolo simple denominado IP encargado de enviar paquetes individuales por la red hacia un nodo de destino, y otro más complicado denominado TCP que se encargará de proveer un control de flujo de los paquetes enviados, asegurando que lleguen a su destino de una forma correcta ordenada. Para aquellas aplicaciones que no requieran un control tan estricto, se creó el protocolo User Datagram Protocol (UDP), que al igual que TCP, utiliza los servicios del protocolo IP, pero sin dar fiabilidad (ver figura 2.1-1 y 2.1-2).

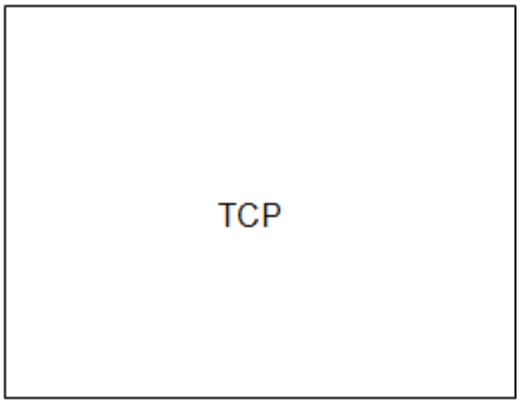


FIG.2.1-1 Primer Diseño TCP/IP

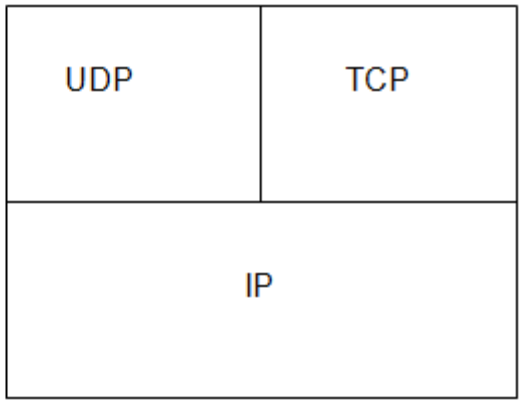


FIG.2.1-2 Estructura Jerárquica

Autor: Investigador
Fuente: G. Verdejo Álvarez: Universidad Barcelona 2000

Durante los últimos años ochenta Internet creció hasta incluir el potencial informático de las universidades y centros de investigación, lo que unido a las posteriores empresas privadas, organismos públicos y asociaciones de todo el mundo supuso un fuerte impulso para Internet que dejó de ser un proyecto con protección estatal para convertirse en la mayor red de computadoras del mundo.

Se trata de una asociación de miles de redes conectadas entre sí. Todo ello da lugar a la RED DE REDES, en la que una computadora de una red puede intercambiar información con otra situado en una red remota.

En gran parte, este espectacular crecimiento se debe a la notable mejora en la facilidad de uso de los servicios ofrecidos, dado que aún manteniéndose los

servicios originales de transferencia de ficheros, correo electrónico o acceso remoto, mediante World Wide Web (www), un servicio de consulta de documentos hipertextuales, ha sido el paso definitivo hacia la popularidad de la que actualmente todos los usuarios pueden tener acceso.

En la actualidad el Internet ha tenido un enorme crecimiento en todas sus herramientas, permitiendo a los millones de usuarios poder comunicarse desde cualquier parte del país como a nivel mundial, como las direcciones de e-mail crecieron de 253 millones en el año 1998 a 1.600 millones en el año 2006. En ese lapso, la cantidad de e-mails enviados creció a una tasa tres veces mayor que las personas que utilizan el e-mail.

El alto rendimiento de Internet a producido un gran porcentaje en los mensajes instantáneos que se estima que existirán 250 millones de cuentas de mensajes instantáneos para el año 2010, incluyendo las cuentas de consumidores hacia donde los mensajes comerciales instantáneos son enviados.

2.1.1 INTERNET EN LA SOCIEDAD

Internet tiene un impacto profundo en el trabajo, entretenimiento a nivel mundial. Gracias a la web, millones de personas tienen acceso fácil e inmediato a una cantidad extensa y diversa de información en línea. Como es el desarrollo y la distribución de colaboración del software de Free/Libre/Open-Source (SEDA) en GNU, Linux, Mozilla y OpenOffice.org.

Internet ha llegado a gran parte de los hogares y de las empresas de los países ricos, en este aspecto se ha abierto una brecha digital con los países pobres, en los cuales la penetración de Internet y las nuevas tecnologías es muy limitada para las personas.

Empresas grandes medianas y pequeñas utilizan el Internet como una herramienta de trabajo, permitiendo comunicarse con otras entidades de trabajo a nivel mundial.

También permite a los estudiantes que puedan realizar carreras en diferentes países como son las maestrías o doctorados, con la posibilidad de tener una guía mediante videoconferencia.

No obstante, en el transcurso del tiempo se ha venido extendiendo el acceso a Internet en casi todas las regiones del mundo, de modo que es relativamente sencillo encontrar por lo menos 2 computadoras conectadas en regiones remotas.

Desde una perspectiva cultural del conocimiento, Internet ha sido una ventaja y una responsabilidad. Para la gente que está interesada en otras culturas, la red de redes proporciona una cantidad significativa de información, imágenes, videos para los investigadores.

Internet entró como una herramienta de globalización, poniendo fin al aislamiento de culturas. Debido a su rápida masificación e incorporación en la vida del ser humano.

2.2 **DESARROLLO DE INTERNET A BASE DE LOS PROTOCOLOS TCP/IP**

Internet es un conglomerado muy amplio y extenso en el que se encuentran computadoras con sistemas operativos incompatibles, redes más pequeñas y distintos servicios con su propio conjunto de protocolos para la comunicación. Ante tanta diversidad resulta necesario establecer un conjunto de reglas comunes para la comunicación entre estos diferentes elementos y que además optimice la utilización de recursos tan distantes. Este papel lo tiene el protocolo TCP/IP y también puede usarse como protocolo de comunicación en las redes privadas intranet y extranet.

Los diferentes protocolos de la suite TCP/IP trabajan conjuntamente para proporcionar el transporte de datos dentro de Internet (o Intranet). En otras palabras, hacen posible que accedan a los distintos servicios de la Red. Estos servicios incluyen, transmisión de correo electrónico, transferencia de ficheros, grupos de noticias, acceso a la World Wide Web.

TCP/IP es la base de Internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo PC, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

La familia de protocolos de Internet puede describirse por analogía con el modelo OSI, que describe los niveles o capas de la pila de protocolos, aunque en la práctica no corresponde exactamente con el modelo en Internet. En una pila de protocolos, cada nivel soluciona una serie de problemas relacionados con la transmisión de datos, y proporciona un servicio bien definido a los niveles más altos. Los niveles superiores son los más cercanos al usuario y tratan con datos más abstractos, dejando a los niveles más bajos la labor de traducir los datos de forma que sean físicamente manipulables.

El modelo de Internet fue diseñado como la solución a un problema práctico de ingeniería. El modelo OSI en cambio fue propuesto como una aproximación teórica y también como una primera fase en la evolución de las redes de computadoras. Por lo tanto, el modelo OSI es más fácil de entender, pero el modelo TCP/IP es el que realmente se usa.

OSI significa Interconexión de sistemas abiertos. Este modelo fue establecido por ISO para implementar un estándar de comunicación entre equipos de una red, estas son las reglas que administran la comunicación entre equipos. De hecho, cuando surgieron las redes, cada fabricante contaba con su propio sistema (es decir de un sistema patentado), con lo cual coexistían diversas redes incompatibles. Por esta razón, fue necesario establecer un estándar.

La función del modelo OSI es estandarizar la comunicación entre equipos para que diferentes fabricantes puedan desarrollar productos (software o hardware) compatibles (siempre y cuando sigan estrictamente el modelo OSI). En la figura 2.2-3 se muestra el modelo OSI con ISO vs TCP/IP.

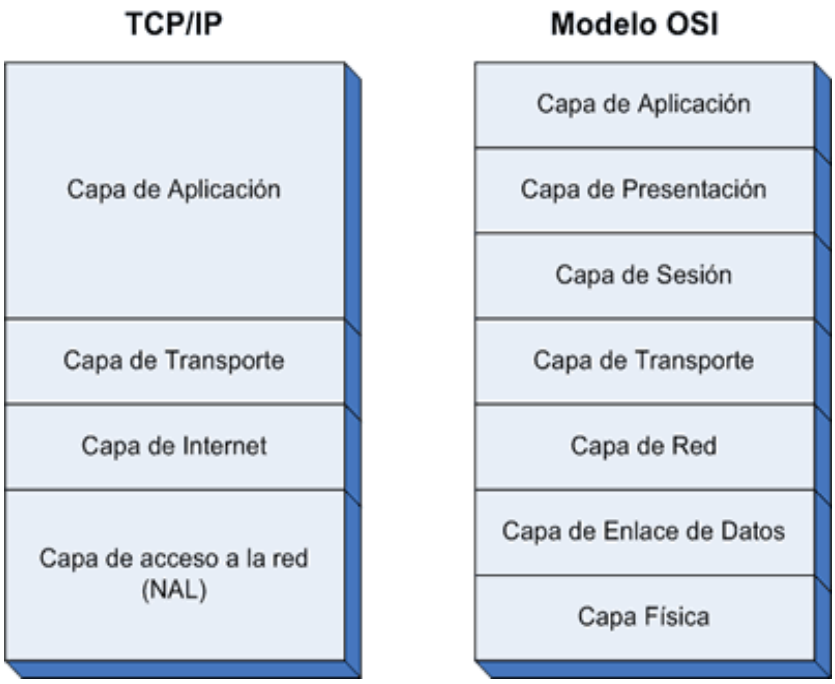


FIG. 2.2-3 Modelo OSI con ISO vs TCP/IP

Autor: Investigador
Fuente: http://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

De esta manera el conjunto TCP/IP está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a Internet y a los servidores web. Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

TCP/IP opera a través del uso de una pila. Dicha pila es la suma total de todos los protocolos necesarios para completar una transferencia de datos entre dos máquinas (así como el camino que siguen los datos para dejar una máquina o entrar en la otra). La pila está dividida en capas, como se muestra en la siguiente tabla (2.2-1):

EQUIPO SERVIDOR O CLIENTE	
Capa de Aplicaciones	Cuando un usuario inicia una transferencia de datos, esta capa pasa la solicitud a la Capa de Transporte.
Capa de Transporte	La Capa de Transporte añade una cabecera y pasa los datos a la Capa de Red.
Capa de Red	En la Capa de Red, se añaden las direcciones IP de origen y destino para el enrutamiento de datos.
Capa de Enlace de Datos	Ejecuta un control de errores sobre el flujo de datos entre los protocolos anteriores y la Capa Física.
Capa Física	Ingresa o engresa los datos a través del medio físico, que puede ser Ethernet vía coaxial, PPP vía módem, etc.

Tabla. 2.2-1 Como Trabaja TCP/IP

Autor: Investigador
Fuente: http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/ip.htm

Después de que los datos han pasado a través del proceso ilustrado en la tabla anterior, viajan a su destino en otra máquina de la red. Allí, el proceso se ejecuta al revés (los datos entran por la capa física y recorren la pila hacia arriba). Cada capa de la pila puede enviar y recibir datos desde la capa adyacente. Cada capa está también asociada con múltiples protocolos que trabajan sobre los datos.

Para transmitir información a través de TCP/IP, ésta debe ser dividida en unidades de menor tamaño. Esto proporciona grandes ventajas en el manejo de los datos que se transfieren y, por otro lado, esto es algo común en cualquier protocolo de comunicaciones.

2.2.1 ESTUDIO DE LAS CAPAS DE LA ARQUITECTURA TCP/IP

El protocolo TCP/IP tiene que estar a un nivel superior del tipo de red empleado y funcionar de forma transparente en cualquier tipo de red. Y a un nivel inferior de los programas de aplicación (páginas WEB, correo electrónico) particulares de cada sistema operativo.

TCP/IP contiene cuatro capas, y cada una de estas capas tiene una función específica. Ver en la figura (2.2-4)

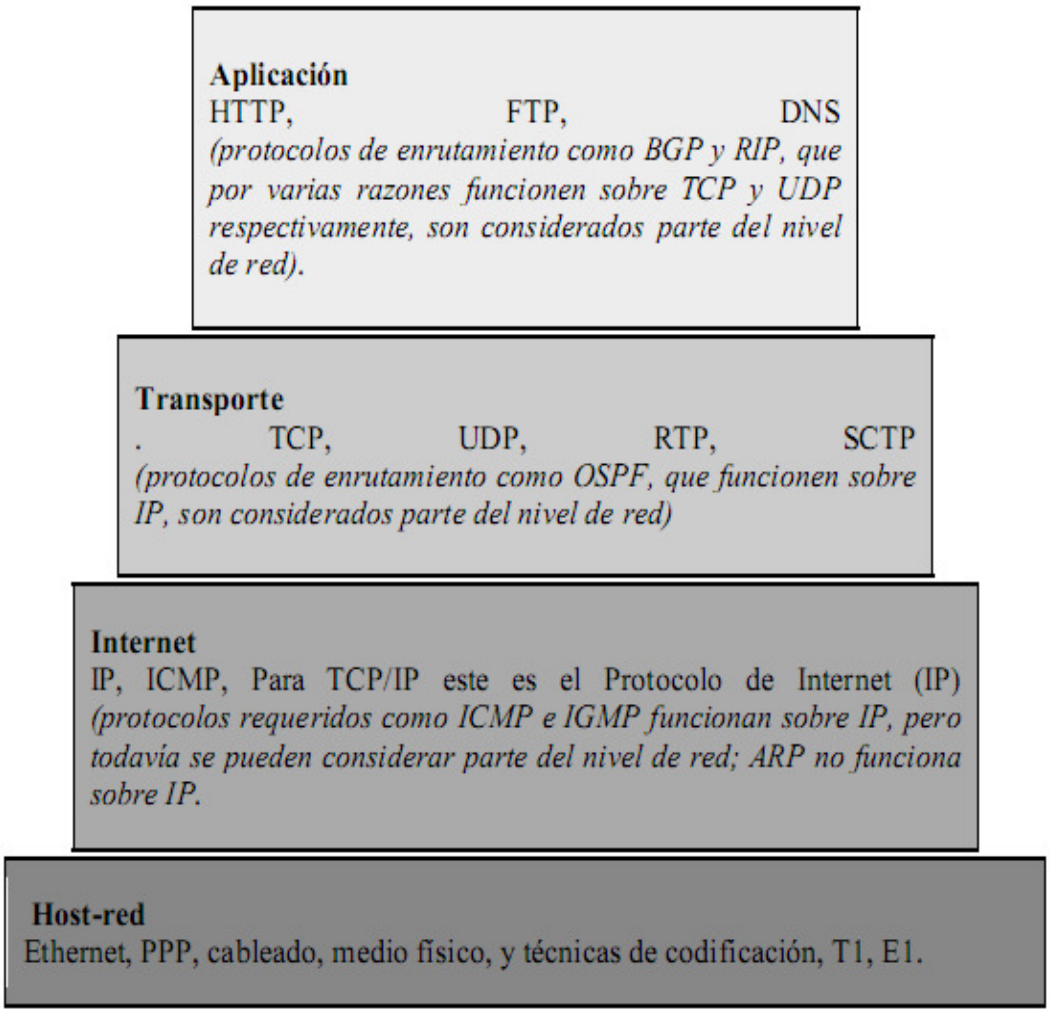


FIG. 2.2-4 Capas de TCP/IP

Autor: Investigador
Fuente: http://www.linuxchile.cl/docs.php?op=imprimirVersion&doc=16&id=1l

Capa de Acceso a la Red (Capa de Datos o Capa de Enlace).

Los protocolos de esta capa proporcionan al sistema los medios para enviar los datos a otros dispositivos conectados a la red. Es en esta capa donde se define como usar la red para enviar un datagrama. Es la única capa de la pila cuyos protocolos deben conocer los detalles de la red física. Este conocimiento es necesario pues son estos protocolos los que han de dar un formato correcto a los datos a transmitir, de acuerdo con las restricciones que se impongan, físicamente, la red

Las principales funciones de los protocolos definidos en esta capa son:

- Encapsulación de los datagramas dentro de los marcos a transmitir por la red.
- Traducción de las direcciones IP a las direcciones físicas de la red

Esta capa incluye los detalles de la tecnología LAN y WAN y todos los detalles de las capas físicas y de enlace de datos del modelo OSI.

Los controladores para las aplicaciones de software, las tarjetas de módem y otros dispositivos operan en la capa de acceso de red que define los procedimientos para realizar la interfaz con el hardware de la red y para tener acceso al medio de transmisión.

Capa de Internet

También conocida como Capa de Red (network layer), es la encargada de mover los paquetes a través de las diferentes redes para llegar a su destino. En esta capa se encuentran los protocolos de más bajo nivel, destacando el IP.

Esta capa tiene como propósito seleccionar la mejor ruta para enviar paquetes por la red. El protocolo principal que funciona en esta capa es el Protocolo de Internet (IP). La determinación de la mejor ruta y la conmutación de los paquetes ocurren en esta capa.

Este protocolo proporciona los servicios básicos de transmisión de paquetes sobre los cuales se construyen todas las redes TCP/IP. Las funciones de este protocolo incluyen:

- Definir el paquete, que es la unidad básica de transmisión en Internet.
- Definir el esquema de direccionamiento de Internet.
- Mover los datos entre la capa de acceso a red y la capa de transporte.
- Encauzar los paquetes hacia sistemas remotos. (Routing)
- Realizar la fragmentación y re-ensamblaje de los datagramas.

El protocolo IP es un protocolo sin conexión, es decir, no intercambia información de control para establecer una conexión antes de enviar los datos. En caso de que dicha conexión fuese necesaria, el IP delegará tal labor en protocolos de otras capas. Este protocolo no realiza detección de errores o recuperación de datos.

Los protocolos que operan en la Capa de Internet son:

- IP: proporciona un enrutamiento de paquetes no orientado a conexión de máximo esfuerzo. El IP no se ve afectado por el contenido de los paquetes, sino que busca una ruta de hacia el destino.
- ICMP: Protocolo de mensajes de control en Internet suministra capacidades de control y envío de mensajes.
- ARP: Protocolo de resolución de direcciones determina la dirección de la capa de enlace de datos, la dirección MAC[13], para las direcciones IP conocidas.
- RARP: Protocolo de resolución inversa de direcciones determina las direcciones IP cuando se conoce la dirección MAC.

[13] **MAC:** Media Access Control es un identificador de 48 bits que corresponde de forma única a una Ethernet de red. También se le conoce como dirección Física

Capa de Transporte

Proporciona un flujo de datos entre dos computadoras. Este flujo de datos puede ser fiable (Transmission Control Protocol, TCP) o no fiable (User Datagram Protocol, UDP).

Esta capa proporciona servicios de transporte desde el host origen hacia el host destino. Permitiendo formar una conexión lógica entre los puntos finales de la red, el host transmisor y el host receptor. Los protocolos de transporte segmentan y re ensamblan los datos mandados por las capas superiores en el mismo flujo de datos, o conexión lógica entre los extremos. La corriente de datos de la capa de transporte brinda transporte de extremo a extremo.

Se suele decir que internet es una nube. La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube. El control de punta a punta, que se proporciona con las ventanas deslizantes y la confiabilidad de los números de secuencia y acuses de recibo, es el deber básico de la capa de transporte cuando utiliza TCP.

La capa de transporte también define la conectividad de extremo a extremo entre las aplicaciones de los hosts.

Capa de Aplicación

Es la encargada de manejar los detalles particulares relativos a las diferentes aplicaciones (WWW, TELNET, FTP).

La capa de aplicación del modelo TCP/IP maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo. El modelo TCP/IP combina todos los aspectos relacionados con las aplicaciones en una sola capa y asegura que estos datos estén correctamente empaquetados antes de que pasen a la capa siguiente. TCP/IP incluye no sólo las especificaciones de Internet y de la capa de transporte, tales como IP y TCP, sino también las especificaciones para aplicaciones comunes. TCP/IP tiene protocolos que soportan la transferencia de archivos, e-mail, y conexión remota, además de los siguientes:

- Telnet: Protocolo que permite la conexión remota de terminales.
- FTP: Utilizado para efectuar transferencias interactivas de ficheros.
- SMTP: Este es el protocolo que permite enviar correo a través de la red.

Estos tres protocolos hacen uso de los servicios orientados a la conexión de TCP. Algunos protocolos que, en cambio, usan los servicios del UDP son:

- DNS: Protocolo que traduce en direcciones IP los nombres asignados a los dispositivos de la red.
- NFS: Protocolo que permite la compartición de ficheros por distintas maquinas de una red.
- RIP: Utilizado por los dispositivos de la red para intercambiar información relativa a las rutas a seguir por los paquetes.

2.3 ANALISIS DEL PROTOCOLO IPv4

La versión utilizada en la actualidad del protocolo IP es la 4, es usada desde 1.981. En la versión 4 del protocolo IP las direcciones están formadas por 4 números de 8 bits (un número de 8 bits en binario equivale en decimal desde 0 hasta 255) que se suelen representar separados por puntos, por ejemplo: **217.76.128.63** Cada dirección IP está conformada por 32 bits agrupados en 4 conjuntos de 8 bits cada uno (octetos). En la Figura 2.3-5 se presenta el formato de las direcciones del Protocolo IPv4.

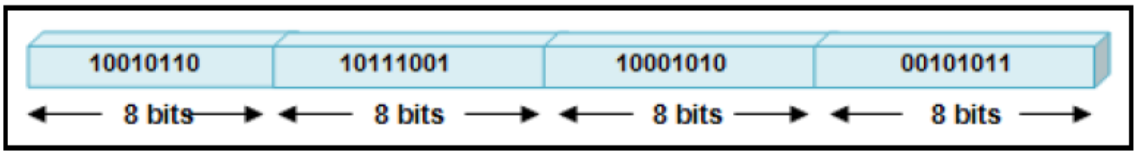


FIG. 2.3-5 Formato de las direcciones IPv4

Autor: Investigador
Fuente: http://www.monografias.com/trabajos30/direccionamientoip/direccionamiento-ip.shtml

En la forma binaria se conforman de cuatro agrupaciones de ocho dígitos cada una (0 y 1), que se determina como $2^8 = 256$.

Esta combinación es capaz de generar aproximadamente 4.000 millones de combinaciones. Esto en un principio puede parecer más que suficiente, en realidad no lo es. Se estima que en la actualidad se encuentran en uso aproximadamente unos 2/3 de estas combinaciones además hay que tener en cuenta que no todas las combinaciones están disponibles para el protocolo IP público (Se utiliza en la conexión con Internet y facilita la ISP).

Este tipo de direccionamiento, permite una gran flexibilidad a la hora de definir redes que están conectadas a Internet. Así una clase A sería ideal para redes muy grandes, ya que permite 128 redes (2^7) de 16.777.216 (2^24) computadoras cada una. Mientras que una clase B permite 16.384 (2^14) redes con 65.535 computadoras, y una clase C permite 2.097.152 (2^21) redes de 256 computadoras.

En principio hay que asegurar una serie de combinaciones diferentes para las conexiones con Internet, por lo que a cada proveedor ISP[14] se le asigna un determinado número de direcciones IP, asignándolas estos a su vez entre sus clientes. Para optimizar este número de conexiones los proveedores ISP recurren al sistema de IP dinámica. Este sistema hace posible que con un número limitado de IP's se atienda a un número bastante superior de usuarios, a condición de que el número de conexiones simultaneas no supere el número de IP's asignadas.

En la versión 4 de los protocolos TCP/IP, estas direcciones cumple dos requisitos básicos:

- Deben ser únicas. No puede haber dos computadoras con la misma dirección.
- Las direcciones son números de 32 bits (4 bytes). Estas direcciones se representan mediante cuatro números decimales separados por un punto

[14] **ISP:** Internet Service Provider. Un proveedor de servicios de una empresa que brinda conexión a Internet a sus clientes.

En la Tabla 2.3-2 y la Figura (2.3-6) se muestran las direcciones con su rango y clases que contiene cada una.

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

Tabla. 2.3-2 Clases de direcciones IP en Internet

Autor: Investigador
Fuente: http://www.monografias.com/trabajos30/direccionamientoip/direccionamiento-ip.shtml

Clase A	0	Identificador de red (7 bits)					Número de ordenador (24 bits)	
Clase B	1	0	Identificador de red (14 bits)				Número de ordenador (16 bits)	
Clase C	1	1	0	Identificador de red (21 bits)			Número de ordenador (8 bits)	
Clase D	1	1	1	0	Identificador de red (28 bits)			
Clase E	1	1	1	1	0	Reservado para futuro uso (27 bits)		

FIG. 2.3-6 Subdivisión de los 32 bits para las clases A, B,C, D, E

Autor: Investigador
Fuente: http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP

Dependiendo del número de hosts que se necesiten para cada red, las direcciones de Internet se han dividido en las clases primarias A, B y C. La clase D está formada por direcciones que identifican no a un host, sino a un grupo de ellos. Las direcciones de clase E no se pueden utilizar (están reservadas)

Al igual que las direcciones numéricas IP, los nombres tienen una jerarquía que permite la resolución de un nombre en su dirección numérica. La resolución del nombre siempre se realiza de derecha a izquierda.

2.3.1 ARQUITECTURA DEL PROTOCOLO IPv4

El formato del protocolo IPv4 del encabezado que viaja actualmente en cada paquete de datos en Internet, es un esquema que puede verse en la figura 2.3-7

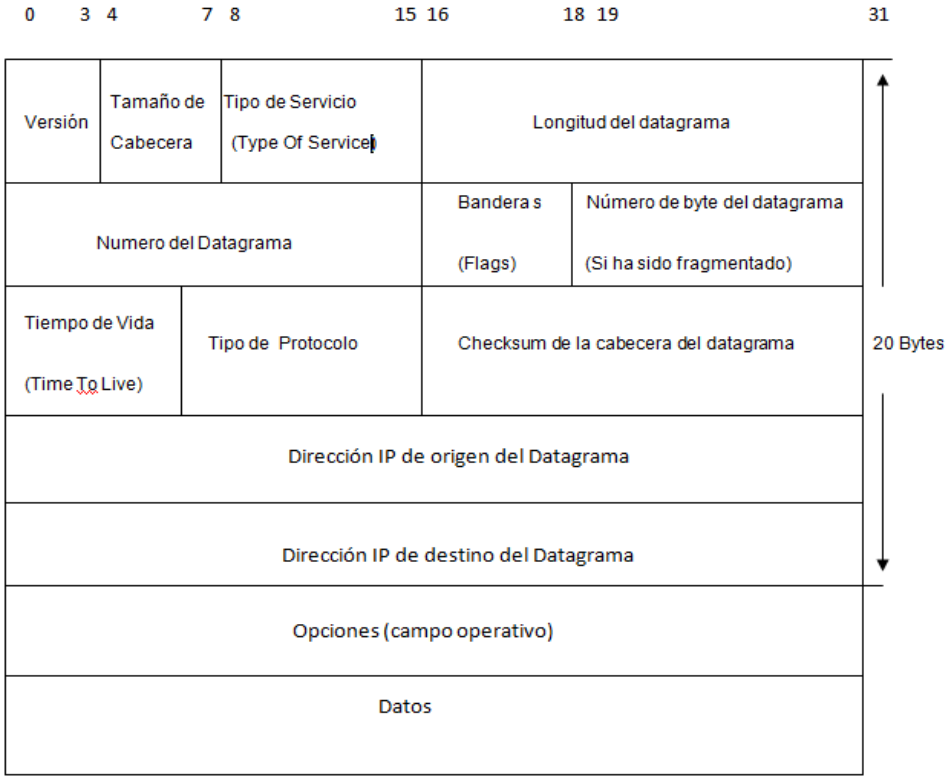


FIG 2.3-7 Estructura de un Datagrama IPv4

Autor: Investigador
Fuente: http: http://www.ipv6.codarec.frm.utn.edu.ar/

NOTA: Esta grafica es modificada por el Investigador

En la figura 2.3-7 se puede ver el formato de un datagrama IP conformado en bloques de 32 bits (4 bytes). El datagrama IP se transmite enviando primero el bit 0, luego el bit 1, 2, 3 y así sucesivamente hasta finalizar el datagrama.

Campo Version (4 bits)

Permite saber si un datagrama es de una misma versión de IP o si necesita alguna conversión cuando se están usando versiones diferentes.

Campo tamaño de la cabecera (Header Length)

Permite saber el tamaño total del encabezado que consta de 20 bytes fijos y hasta 40 bytes de opciones.

Campo del tipo de servicio (Type Of Service)

El tipo de servicio determina la política a seguir en el envío del datagrama por Internet. Las opciones posibles son minimizar el retraso, maximizar el rendimiento, maximizar la fiabilidad del transporte y minimizar el coste económico del transporte.

Campo longitud del datagrama

Indica la longitud total del datagrama incluyendo encabezado y datos. Este valor es muy importante, ya que permite saber que tamaño de memoria se debe reservar para la recepción del datagrama. Además indica el número de bytes a leer, lo que permite un simple control de error.

Campo número de identificación del datagrama

Es un número de 16 bits que en caso de fragmentación de un datagrama indica su posición en el datagrama original. Esto permite recomponer el datagrama original en la máquina de destino.

Su especificación está recopilada del RFC791

Campo banderas (Flags)

Son 3 bits. El primero permite señalar si el datagrama recibido es un fragmento de un datagrama mayor, bit M (More) activado. El segundo especifica si el datagrama no debe fragmentarse, bit DF (Don't fragment) activado. Y el tercero no se utiliza actualmente, asignándole el valor 0.

Campo número de byte en el datagrama

Indica la posición en bytes que ocupan los datos en el datagrama original. Sólo tiene sentido si el datagrama forma parte de uno mayor que ha sido fragmentado. De esta forma se puede reconstruir el datagrama original con los fragmentos.

Campo tiempo de vida

Es un campo de 8 bits que indica el tiempo máximo que el datagrama será válido y podrá ser transmitido por la red. Esto permite un mecanismo de control para evitar datagramas que circulen eternamente por la red (por ejemplo en el caso de bucles). Este campo se inicializa en la computadora de origen a un valor (máximo 2^8 = 256) y se va decrementando en una unidad cada vez que atraviesa un router. De esta forma, si se produce un bucle y no alcanza su destino en un máximo de 255 "saltos", es descartado. Entonces se envía un datagrama ICMP de error al computador de origen para avisar de su pérdida.

Campo tipo de protocolo

Es un valor que indica a que protocolo pertenece el datagrama (TCP, UDP, ICMP). Es necesario debido a que todos los servicios de Internet utilizan IP como transporte, lo cual hace necesario un mecanismo de discriminación entre los diferentes protocolos.

Campo checksum de la cabecera del datagrama (Header Checksum)

Su función es simplemente la de un mecanismo de control de errores. De esta forma, si se encuentra un error en el checksum de un datagrama IP, este es simplemente descartado y no se genera ningún mensaje de error. Esto implica que es deber de las capas superiores el control del flujo de los datagramas

asegurándose que estos lleguen correctamente al destino, ya sea utilizando un protocolo fiable (TCP) o implementando internamente algún tipo de control.

Campo direcciones IP de origen como la de destino (IP address)

Indican la dirección IP única a nivel mundial del nodo origen y nodo destino. Las direcciones IP son administradas a nivel mundial por el NIC y para poder usarlas se necesita solicitarlas y registrarlas.

Campo de opciones

Estos octetos se dejaron sin especificar con el objeto de darles significado cuando el protocolo tuviera más necesidades. Se han especificado algunas opciones como son paquetes con seguridad, rutas de entrega estricta o sugerida, registro de rutas y registro de tiempos de travesía.

2.4 SEGURIDADES DEL PROTOCOLO TCP EN IPv4

Se define comunicación como un intercambio de información. Así mismo se define una red (Network) como un mecanismo físico que permite la comunicación entre dos o más computadoras separadas entre sí mediante el uso de un protocolo común.

Desde el mismo momento en que se conectan a una red (ya sea una red local en una empresa o desde Internet), no se deja de enviar y recibir información. Esta información circula por la red de forma que el destinatario pueda recibirla y enviar una respuesta en caso necesario. Cuando se tiene dos o más computadoras están conectados a una misma red, existe la posibilidad de estas computadoras puedan acceder a esta información, e incluso a los otros computadores conectados.

Desde el mismo momento en que interesa que una información no sea pública (sea cual sea el motivo) se necesita controlar el acceso a toda información para decidir si debe ser pública o se debe protegerla mediante sistemas de seguridad.

La necesidad de seguridad siempre viene precedida de una amenaza (justificada o no).

Una red donde millones de computadoras intercambian innumerable cantidad de información mediante el envío y recepción de datagramas según el conjunto de protocolos TCP/IP se puede distinguir tres cualidades básicas deseables en toda comunicación:

- Secreta. No solo respecto al contenido de la información enviada/recibida, sino también al origen y destino de la información.
- Auténtica. Los datos no han sido modificados, provienen del origen legítimo (no hay suplantación de un usuario por otro y no pueden ser repudiados) y son ciertos en el momento de su recepción (evitar reutilización de la información).
- Accesible. Tanto el emisor como el receptor han de poder intercambiar información cuando sea necesario.

Las amenazas a su vez pueden ser clasificadas principalmente en cuatro grupos distintos:

- Interrupción. El acceso a un recurso/comunicación se ve interrumpido ya sea físicamente (destrucción de la red...) o lógicamente (se modifica localización, los derechos de acceso).
- Intercepción. Alguien no autorizado consigue tener acceso al recurso/comunicación.
- Modificación. Obtención no sólo de acceso no autorizado al recurso/comunicación, sino también de la capacidad de modificarlo (modificación de los datos enviados/recibidos entre dos máquinas).
- Fabricación. Además de conseguir acceso al recurso/comunicación, se tiene la posibilidad de insertar información falsa.

Es necesario tener seguridad en las redes como en los protocolos para que la información transmitida sea fiable, segura y no tenga amenazas que puedan ser un problema para los usuarios.

2.4.1 SEGURIDADES DE INTERNET BAJO IPV4

Después de analizar brevemente las posibilidades de que una comunicación sea atacada, se concluye fácilmente que la seguridad debe ser un pilar básico en cualquier tipo de intercambio de información, y por tanto la comunicación a través de Internet no debería ser una excepción.

Desde los inicios de Internet y hasta finales de los años 90, casi toda la información que circulaba por Internet no utilizaba ningún tipo de cifrado, atravesando todas las máquinas que encontraba hasta en destinatario tal y cómo había sido enviada. Esto se debía principalmente a que en un principio el carácter divulgativo y científico de ARPANET lo hacía sólo accesible a ciertas universidades y laboratorios de investigación, motivo que propició que en las definiciones de los diferentes protocolos (TCP, UDP, IP) de esos años, no se contemplase ninguna posibilidad de seguridad, ni tan sólo en los protocolos de nivel superior (cuando se realiza un Telnet a una máquina remota, el password circula tal cual, sin ningún tipo de cifrado o sistema de seguridad).

Posteriormente su expansión hacia el carácter lúdico y el público en general, hizo que el número de usuarios (así como sus fines) creciera exponencialmente. La proliferación de robos realizados por desaprensivos que aprovechaban las debilidades de unos protocolos diseñados sin ninguna seguridad, empezó a inundar los medios informativos, haciendo que la opinión pública (en algunos países más que otros) exigiera un fin de estas actuaciones.

Esto obligó a los diseñadores de protocolos a añadir algunos parches y extensiones de emergencia a unos protocolos que no habían sido diseñados para ello.

De forma paralela el comercio electrónico (e-comerce) se empezaba a desarrollar, y diferentes soluciones fueron adoptadas por las empresas implicadas. Todas estas soluciones siempre se englobaron en las capas superiores de los protocolos (TCP).

2.4.2 SEGURIDADES EN LAS CAPAS

Tal y como se ha comentado en los puntos anteriores, la seguridad en la versión 4 de IP no fue contemplada en su diseño original, con lo que al querer introducir ampliaciones en las especificaciones IP (IP versión 5) se encontraron muchos problemas, entre ellos la gran cantidad de software que debía modificarse para adoptar esta ampliación debido al gran tamaño que ya tenía Internet. Además se tardó mucho tiempo en finalizar las nuevas especificaciones, a medida que se fue desarrollando el comercio electrónico (e-comerce) las empresas que vendían su producto por Internet no podían modificar ninguno de los protocolos (IP, TCP, UDP) en vista de este inconveniente se fue desarrollando en los niveles la posibilidad de modificar los protocolos correspondientes en la capa de aplicacion (ver figura 2.4-8).

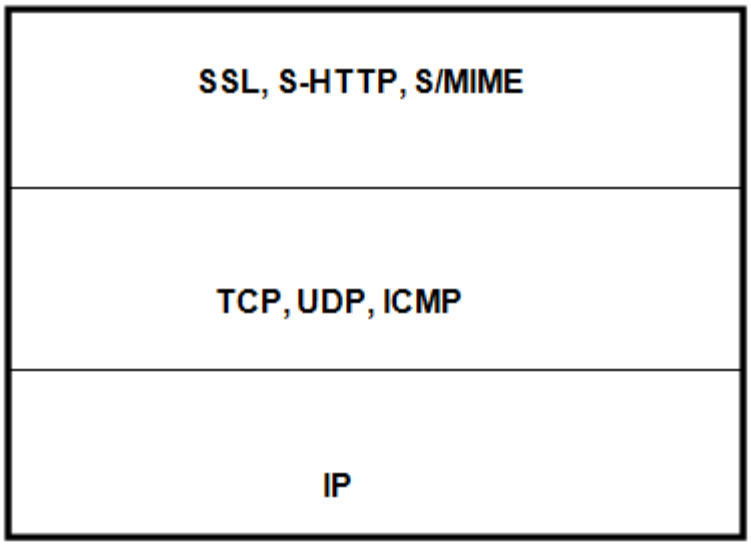


FIG.2.4-8 Ubicación de los Protocolos en las capas superiores

Autor: Investigador
Fuente: http://www.linuxchile.cl/docs.php?op=imprimirVersion&doc=16&id=1I

A continuación se detallan unos ejemplos de soluciones de seguridad adoptadas unánimemente en Internet.

- SSL (Secure Socket Layer) es un protocolo ampliamente utilizando que se basa en una arquitectura de tipo cliente/servidor y que permite una comunicación segura entre dos aplicaciones. Este protocolo permite la negociación de un algoritmo de cifrado y de las claves necesarias para asegurar un canal de seguridad donde viaja la información (Channel Security) entre el cliente y el servidor. Este canal tiene tres propiedades principalmente:

    1. El canal garantiza la privacidad. Después del negociado de la clave privada todos los mensajes son cifrados.

    2. El canal garantiza la autenticidad. El servidor siempre se autentifica mientras que los clientes pueden hacerlo o no.

    3. El canal garantiza la fiabilidad. Los mensajes incluyen una integridad proporcionada por el uso del sistema MAC.

- S-HTTP (Secure Hypertext Transfer Protocol) es una extensión del protocolo HTTP utilizado en el servicio WWW que proporciona seguridad en el intercambio de documentos multimedia. Proporciona servicios de confidencialidad, autenticidad, integridad y no repudio (poder demostrar a una tercera persona que la información recibida proviene realmente del emisor). Asimismo permite múltiples algoritmos de cifrado (DES, DESX, IDEA y RC2)[15] y de intercambio de claves (RSA, Kerberos, Out-band e In-band).[16]

---

[15] **DES:** Algoritmo de cifrado es decir, un método para cifrar información.
IDEA: En criptografía, International Data Encryption Algorithm es un cifrado por bloques de 64 bytes.
RC2: El RC2 es un algoritmo de cifrado por bloques de clave de tamaño variable.

[16] **RSA:** Es un sistema criptográfico de clave pública es el algoritmo mas utilizado y es válido tanto para cifrar como para firmar digitalmente.

- S/MIME (Secure/Multipurpose INTERNET Mail Extensions) es una extensión del protocolo MIME que añade las características de firma digital y cifrada. Los mensajes electrónicos constan de una cabecera dónde se especifican todas las opciones junto con el origen/destinatario del mensaje.
- SET (Secure Electronic Transaction) es un protocolo desarrollado por las empresas VISA [WWW30] y MASTERCARD [WWW21] para las transacciones electrónicas (e-comerce). Soporta los protocolos DES y RSA para el intercambio de claves y el cifrado de datos, además proporciona los siguientes servicios:

    1. Transmisiones confidenciales.
    2. Autenticación de los dos usuarios.
    3. Comprobación de la integridad en los pagos y las cantidades.
    4. Autenticación cruzada (del comerciante ante el usuario y del usuario al comerciante).

2.5 ANALISIS DEL PROTOCOLO IPv6

Desde hace varios años está planteado el problema del agotamiento de números de IP en su versión IPv4, por lo que la IETF inició un proceso para diseñar una nueva versión del protocolo. Esta versión de IP "nueva generación" vio la luz hace unos años. Pero su implantación se va retrasando al encontrarse algunos mecanismos para rescatar espacio de direcciones en IPv4. En cualquier caso, el futuro de IP está ya definido.

Algunos informáticos se preguntan ¿Porqué no IPv5?, estas direcciones fueron extensiones experimentales y no se acabaron de formalizarse en una nueva versión del protocolo, con lo que para evitar posibles conflictos de numeración y/o confusión, se optó por elegir el número de versión 6.

Como se describe en la RFC 2460, IPv6 es el sustituto de IPv4. Aumenta el tamaño de las direcciones de IP de 32 a 128 bits, lo que da un total de 340.282.366.920.938.463.463.374.607.431.768.211.456 direcciones.
Este aumento en el espacio de direcciones no sólo proporciona mayor número de hosts, sino una jerarquía de direcciones mayor. Según “Christian Huitima (vocero del IETF) estima que habrá 1500 direcciones IPv6 por cada metro cuadrado de la superficie terrestre”.

Teniendo en cuenta que el proceso de transición desde IPv4 va a ser largo, y que ambos protocolos van a tener que coexistir durante mucho tiempo, se ha procurado que no exista dependencia alguna en el proceso de migración a IPv6.

Actualmente se utiliza con más frecuencia la versión 4 del Protocolo de Internet, el aumento de usuarios, aplicaciones, servicios y dispositivos está provocando la migración a una nueva versión, en la siguiente Tabla 2.5-3 se realiza la comparación IPv6 vs IPv4

IPV6	IPV4
Direcciones de 128 bits (16 bytes) de longitud	Direcciones de 32 bits (4 bytes) de longitud
IPSec no es opcional	IPSec es opcional
Configuración automática	Configuración manual
Multicast y anycast	Broadcast
Seguridad obligatoria	Seguridad opcional

Tabla. 2.5-3 IPv6 vs IPv4
Autor: Investigador
Fuente: http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

Principales diferencias entre IPv4 e IPv6

- **Mayor espacio de direcciones**: el tamaño de las direcciones IPv4 cambia de 32 bits a 128 bits, para soportar más niveles de jerarquías de direccionamiento y más nodos direccionales.

- **Simplificación del formato del Header**: algunos campos del Header IPv4 se eliminan o se hacen opcionales.

- **Paquetes IPv6 eficientes y extensibles**: sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesamiento por parte del router.

- **Posibilidad de paquetes con carga útil (datos)**: IPv6 tiene la capacidad de enviar paquetes de hasta 65.355 bytes.

- **Seguridad en el núcleo del protocolo (IPsec):** el soporte de IPsec es un requerimiento del protocolo IPv6.

- **Capacidad de etiquetas de flujo**: puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como la calidad de servicio o el servicio de tiempo real como la video conferencia.

- **Autoconfiguración:** la autoconfiguración de direcciones es más simple. Especialmente en direcciones Globales Unicast, los 64 bits superiores son asignados por un mensaje desde el router y los 64 bits más bajos son asignados con la dirección MAC. En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es más simple.

- **Renumeración:** facilitando el cambio de proveedor de servicios.

- **Características de movilidad**: es la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.

- **Calidad de servicio (QoS)** y clase de servicio **(CoS).**

- Capacidad de Autenticación y Privacidad

Características propias de IPv6:

- **Movilidad.-** IPv6 trae numerosas y significativas mejoras respecto a IPv4, uno de los aspectos en el que se obtienen importantes beneficios será la movilidad. En este sentido, cada vez más se necesita que la comunicación pueda llevarse a acabo en cualquier momento y lugar con un óptimo grado de operatividad, así como de forma transparente al usuario al realizar su propia gestión y control.

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

- **Extensibilidad de Direcciones**.- IPv6 incrementa el tamaño de las direcciones de 32 bits (IPv4) a 128 bits, para soportar más niveles en la jerarquía de direccionamiento, un número mayor de nodos direccionables, y un sistema de autoconfiguración de direcciones.

Se añade un nuevo tipo de dirección, la llamada anycast, de forma que es posible enviar un paquete a cualquier nodo entre un grupo de ellos.

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

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

Rutinas de Seguridad

El protocolo IPv6 introduce rutinas específicas para la encriptación y autenticación de los diferentes niveles de paquetes, la aplicación de ellos solamente depende de que estas funciones estén disponibles.

El método de encriptación codifica los paquetes de datos para prevenir la lectura de los mensajes por personas no autorizadas. La autenticación verifica que la dirección de donde fue enviado en mensaje no se pierda y el paquete de información no sea interferido en la ruta.

Este protocolo permite encriptar y autenticar no solo los paquetes de datos sino también toda la comunicación entre los diferentes anfitriones (HOST), además el usuario puede utilizar el algoritmo estándar de seguridad o solicitar el uso de algoritmos adicionales cuando estén disponibles.

2.5.1 ARQUITECTURA DEL PROTOCOLO IPv6

Esta nueva revisión del protocolo IP se numera con la versión 6. La nueva cabecera del protocolo IP versión 6 (ver figura 2.5-9) no es más que una evolución de la anterior versión. No se han introducido grandes cambios de contenido o estructura, sino que simplemente se ha mejorado y optimizado con los conocimientos y experiencias adquiridas durante los últimos 20 años. Se han suprimido algunos campos redundantes u obsoletos y se han ampliado algunas características para hacer frente a las nuevas necesidades de los usuarios (comunicaciones en tiempo real, seguridad).

La cabecera de un paquete IPv6 es, sorprendentemente, más sencilla que la del paquete IPv4 y además la funcionalidad del protocolo IPv6 es mucho mayor. La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o lenght. Sin embargo, para simplificar la vida de los routers, IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos

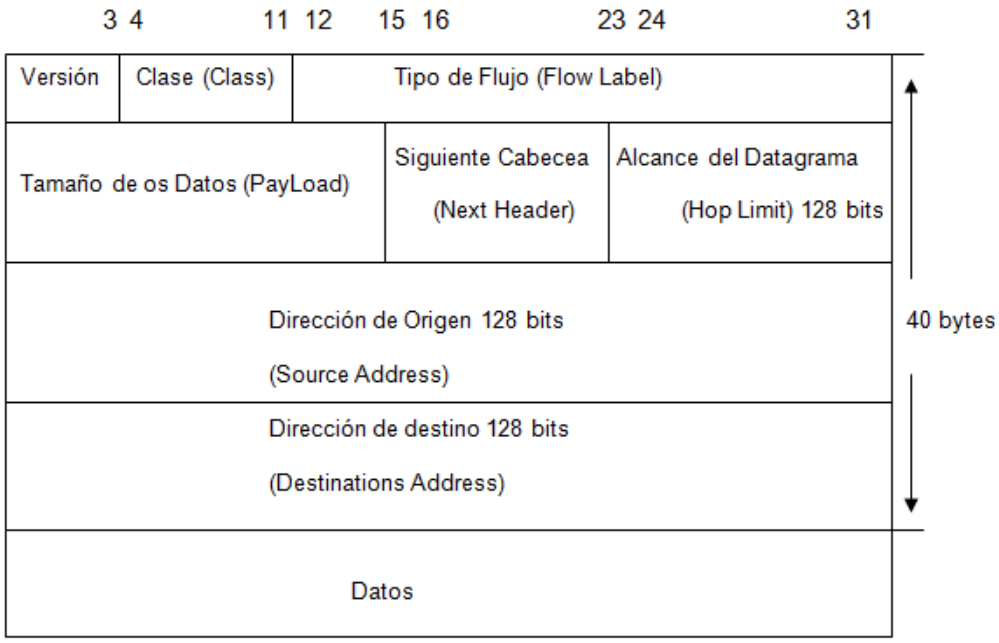


FIG.2.5-9 Estructura de un Datagrama IPv6

Autor: Investigador
Fuente: http://neutron.ing.ucv.ve/revistae/No5/IP%20versi%C3%B3n%206.htm

NOTA: Esta grafica es modificada por el Investigador

Se han suprimido seis campos (tamaño de cabecera, tipo de servicio, número de identificación del datagrama, banderas, número de byte del datagrama fragmentado y el checksum) respecto la versión 4 del protocolo IP. Además se han redefinido los campos de longitud del datagrama, tiempo de vida y de tipo del protocolo.

Campo versión (4 bits)

Se sigue manteniendo como el primer campo del datagrama. Esto es así para mantener la compatibilidad con formatos anteriores y porque permite de una forma sencilla y rápida discriminar que versión de datagrama se recibe, facilitando a los routers el proceso de discriminar entre versión 4 y versión 6.

Campo clase (Class)

Es un número de 8 bits que hace referencia a la prioridad del datagrama. Este campo es una de las nuevas aportaciones para conseguir algunos tipos de aplicaciones (videoconferencia, telefonía, etc) puedan realizarse en tiempo real.

Campo tipo de flujo (Flow Label)

Se compone de 16 bits, que permiten especificar que una serie de datagramas deben recibir el mismo trato. Esto es aplicable por ejemplo a una serie de datagramas que van del mismo origen al mismo destino y con las mismas opciones. Junto con el campo de clase permiten aplicaciones en tiempo real.

Campo tamaño de los datos (Payload Length)

Al igual que en la versión 4, es un número de 16 bits, lo que permite un tamaño máximo en principio de 2^16 = 65536 bytes (64K). No obstante, a diferencia de la versión 4, este número hace referencia sólo al tamaño de los datos que transporta, sin incluir la cabecera

Campo siguiente cabecera (Next Header)

Es un valor de 8 bits que indica al router si tras el datagrama viene algún tipo de extensión u opción.

Este campo substituye al campo de banderas (flags) de la versión 4. De esta manera, en lugar de complicar la cabecera IP con la interpretación de los diferentes bits de opciones, se sitúan fuera del datagrama básico.

Campo alcance del datagrama (Hop Limit)

Este campo es necesario para evitar que los datagramas circulen infinitamente por la red, eliminándose al llegar a 0 (su valor máximo es de 2^8 = 256).

Es un número de 8 bits que indica el número máximo de routers que puede atravesar un datagrama hasta llegar a su destino y es el equivalente al tiempo de vida (TTL) de la versión 4. Cuando un datagrama llega a un router y es encaminado hacia otro computador el alcance del datagrama es decrementado en una unidad.

2.5.2 CABECERA DEL PROTOCOLO IPv6

Tal y como se ha comentado en el punto 2.5.1, la cabecera IP versión 6 no contiene ningún tipo de opciones a diferencia de la versión 4. No obstante, en algunos casos se hace necesario poder especificar algunas características especiales a los routers intermedios para que traten el datagrama IP de una forma determinada. No todos los datagramas son datos que circulan de un usuario a otro por Internet algunos son mensajes entre los diferentes routers

La cabecera de encaminamiento

Con la cabecera de encaminamiento se consegue la funcionalidad equivalente de IPv4 de Source-Routing, es decir, especificar los nodos intermedios por los que ha de pasar el paquete.
Utiliza un sistema de cadena dónde se pueden especificar múltiples cabeceras
En la figura 2.5-10 se muestra la cabecera de encaminamiento.

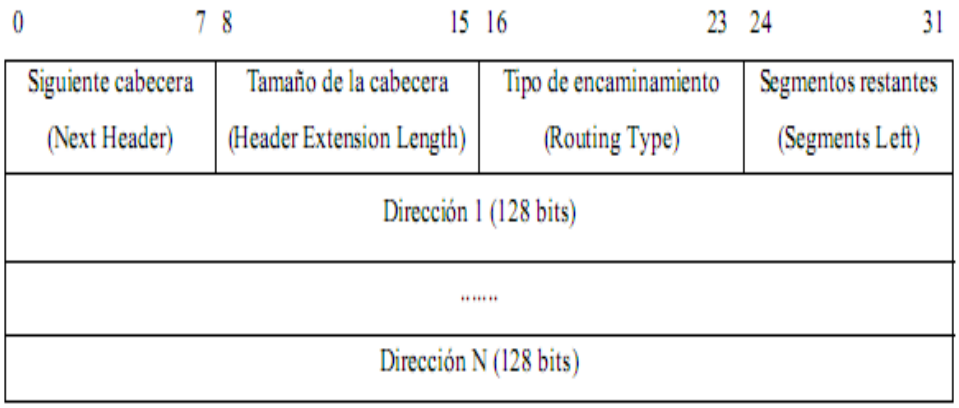


FIG.2.5-10 Cabecera de Encaminamiento

Autor: Investigador
Fuente: http://www.utp.edu.co/php/revistas/ScientiaEtTechnica/docsFTP/111011320-325.pdf

La cabecera de fragmentación

En la versión 6 se diferencia respecto a la de la versión 4 en que no existe un bit de fragmentación, ya que no se fragmentan los datagramas. Si un router recibe un datagrama de tamaño superior al que puede enviar, lo fragmentaba en varios datagramas de menor tamaño. Estos datagramas se encaminaban independientemente, y por lo tanto, si uno sólo de ellos no llegaba a su destino o llegaba incorrecto, todo el datagrama original se desechaba y debía ser retransmitido. Ver la figura 2.5-11 la cabecera de fragmentación.

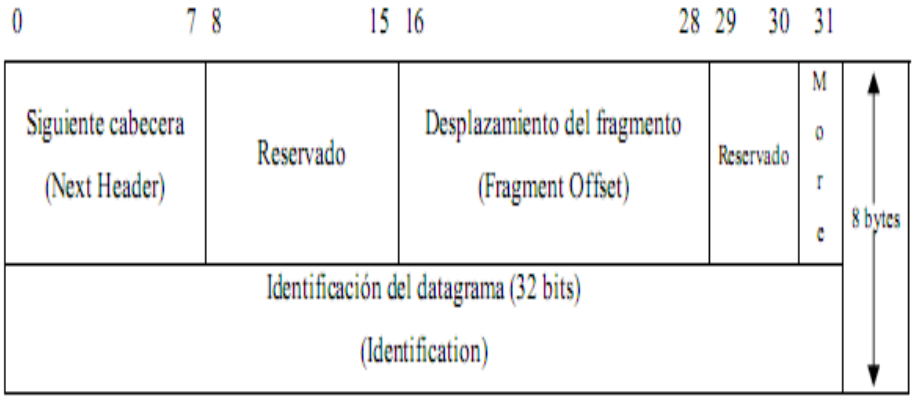


FIG.2.5-11 Cabecera de Fragmentación de datagramas

Autor: Investigador
Fuente: http://www.freebsd.org/doc/es/books/handbook/network-ipv6.html

La cabecera de opciones de destino

Permite añadir opciones extra a los datagramas (ver figura 2.5-12) para que sean procesadas únicamente por el destinatario. Con este formato se permite que aquellos routers intermedios que no necesiten interpretarlas puedan evitarlas sin perder tiempo de proceso.

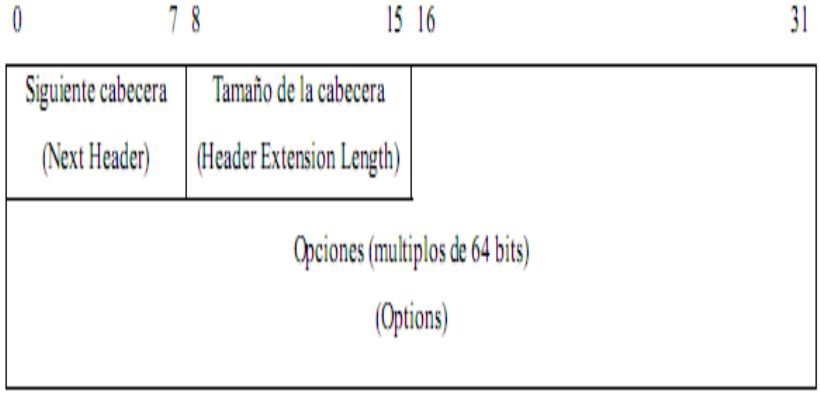


FIG.2.5-12 Cabecera de opciones de destino

Autor: Investigador
Fuente: http://www.freebsd.org/doc/es/books/handbook/network-ipv6.html

La cabecera de opciones entre saltos

Permite especificar opciones que serán procesadas por todos los routers intermedios. Cuando un datagrama llega una cabecera extra, especifica en el datagrama que tipo de cabecera le sigue con un código numérico

La cabecera de autenticación

Es una de las novedades más importantes en la versión 6 del protocolo IP (ver figura 2.5-13) La presencia de una cabecera de autenticación no modifica de ninguna manera el comportamiento del resto de protocolos de nivel superior como TCP o UDP. Esta cabecera tan solo proporciona una seguridad implícita del origen del datagrama. De esta forma los protocolos superiores deben rechazar los paquetes que no estén adecuadamente autenticados.

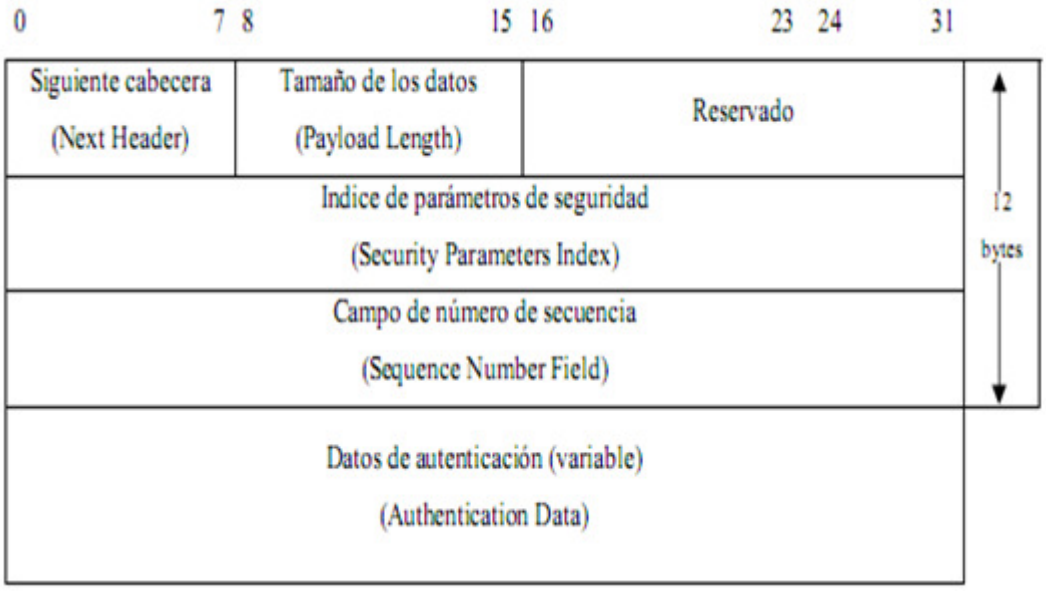


FIG.2.5-13 Cabecera de autentificación IPv6

Autor: Investigador
Fuente: http://www.utp.edu.co/php/revistas/ScientiaEtTechnica/docsFTP/111011320-325.pdf

Tal y como se ha visto, un datagrama puede incluir más de una cabecera. Esto no debería suponer ningún problema para los routers intermedios encargados de encaminarlo hasta su destino. De esta forma, las cabeceras son procesadas por los routers a medida que estas llegan, sin ineficiencias. Es importante señalar que hay algunas cabeceras con mayor importancia que otras, como la cabecera de autenticación que obliga a descartar todo el datagrama si es incorrecta o la cabecera de fragmentación que obliga al re ensamblamiento de datagramas.

Tiene el orden de las diferentes cabeceras que son importantes, y pese a no existir un formato rígido para establecer este orden, hay una recomendación en cuanto al orden adecuado de estas:

- Cabecera IP versión 6 (IPv6 Header).
- Cabecera de opciones entre saltos (Hop-by-hop Options Header).
- Primera cabecera de opciones de destino (Destination Options Header).
- Cabecera de encaminamiento (Routing Header).
- Cabecera de fragmentación (Fragment Header).
- Cabecera de autenticación (Authentication Header).

- Segunda cabecera de opciones de destino (Destination Options Header).
- Cabecera de protocolo de nivel superior.

2.5.3 DIRECCIONAMIENTO IPv6

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

UNICAST:

Identifica una única interfaz. Un paquete enviado a una dirección Unicast es entregado sólo a la interfaz identificada por dicha dirección. El tipo de direccionamiento Unicast se muestra en la Figura 2.5-14

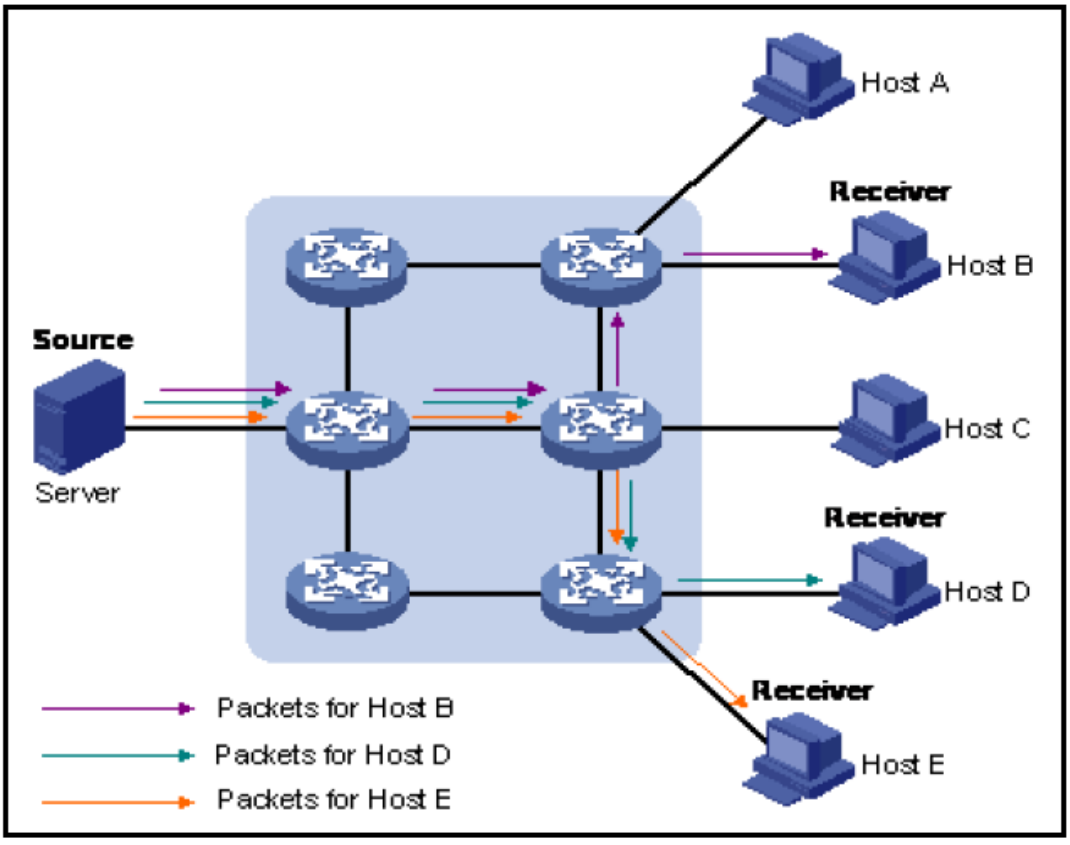


FIG.2.5-14 Direccionamiento Unicast IPv6

Autor: Investigador
Fuente: Ghislayae Xiomara Vera: Universidad de Loja-Zamora 2009

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

- **Link-Local (Local de Enlace):** Se la utiliza para comunicaciones en el mismo enlace. Empiezan todas por **fe80::/10** Se crearon con propósitos de autoconfiguración, descubrimiento de vecinos (no atraviesan los routers).

- **Site-Local (Local de Sitio):** Para comunicaciones y identificar interfaces en el mismo sitio (pueden atravesar routers de un mismo lugar). La definición de "sitio" es un tanto genérica, pero en principio es el área topológica de red perteneciente a un edificio o un campus, perteneciente a una misma organización. Empiezan por **fec0::**./10

- **Global:** Para comunicaciones con servicios públicos. Estas direcciones se pueden utilizar en Internet. Una dirección global empieza **3ffe::** Este tipo de dirección es usada en una organización basada en tres niveles:

    - Topología pública: Asociada a los proveedores y pasarelas de la red troncal asociada a la Internet
    - Topología de sitio: Propia de la red interna de la organización
    - Identificador de interfaz: Asociado con la interfaz de enlace. Según el RFC-2373 existen los siguientes prefijos reservados:

  En la tabla 2.5-4 se muestra los prefijos reservados de la dirección Unicast global.

  Un ejemplo de dirección Unicast es: **3ffe:38e1:0100:a001::,**

Tipo	Prefijo Binario	Prefijo en hexa	Fracción de espacio de direcciones
Reservado para NSAP	0000 001	02* 03*	1/128
Reservado para IPX	0000 010	06* 07*	1/128
Direcciones globales Unicast "aggregatable"	001	2* 3*	1/8
Direcciones enlace-local (**)	1111 1110 10	fe8* .... feb*	1/1024
Direcciones enlace-red (**)	1111 1110 11	fec* .... fef*	1/1024
Direcciones Multicast	1111 1111	ff*	1/256

* => resto puede tomar cualquier valor, pero existen por ahora asignaciones limitadas

(**) No pueden traspasar ruteadores ni pasarelas

Tabla. 2.5-4 Prefijos reservados de la dirección Unicast global

Autor: Investigador
Fuente: http://fmc.axarnet.es/tcp_ip/tema-03/tema-03.htm

MULTICAST:

Identifica un conjunto de interfaces. Un paquete enviado a una dirección multicast es entregado a todas las interfaces del conjunto identificadas con dicha dirección, el esquema del direccionamiento Multicast se presenta en la Figura 2.5-15

Las direcciones Multicast se forman mediante el prefijo **ffxy:: /16**

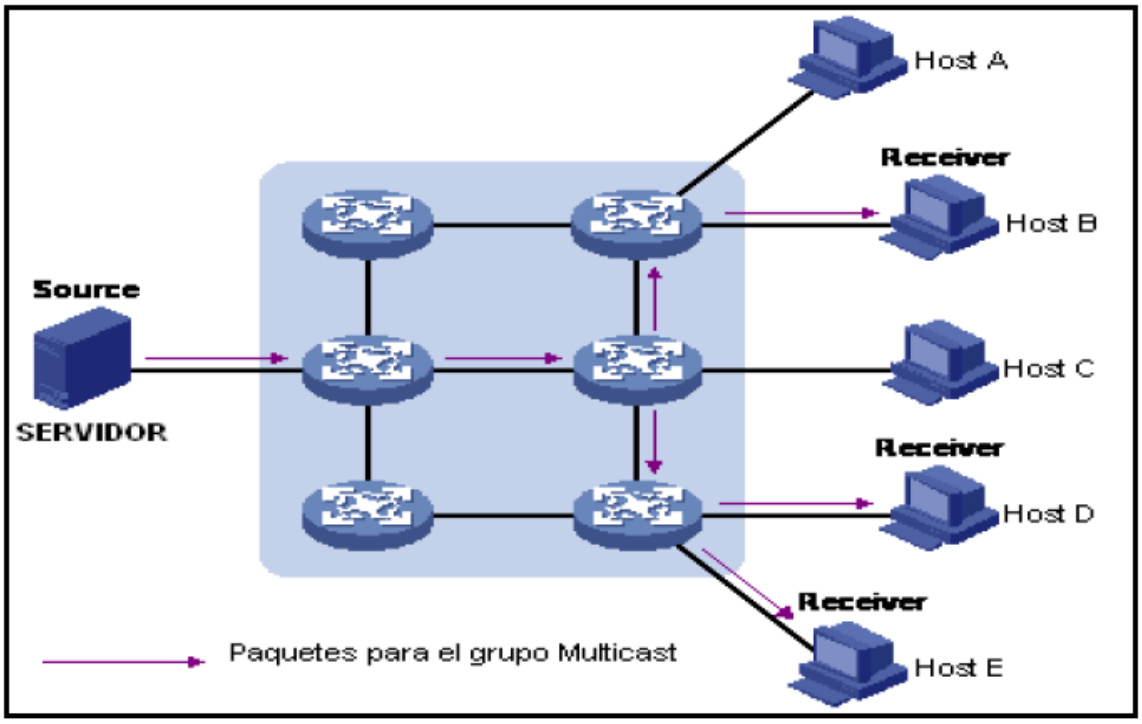


FIG.2.5-15 Direccionamiento Multicast IPv6

Autor: Investigador
Fuente: Ghislayae Xiomara Vera: Universidad de Loja-Zamora 2009

El identificador de grupo asocia a un grupo en particular de interfaces, como ejemplo de direcciones son:

ff01::101 A todos los identificadores de tiempo con identificado de grupo 101 en ámbito del nodo

ff02::101 A todos en el mismo enlace asociado con la misma interfaz con id-grupo 101

ff01::101 A todos en el mismo enlace asociado con la misma interfaz con id-grupo pero a toda la Internet.

ff15::101 No permanente asociada al sitio. La dirección temporal tiene solo sentido a nivel local.

Si el bit T=0 la dirección multicast es permanente y está designada por la ipv6 global address, caso contrario su valor es T=1 y se trata de una dirección temporal. Los cuatro bits del ámbito tiene el siguiente significado.

0	Reservado
1	Ámbito local de Nodo
2	Ámbito local de Enlace
3	No asignado
4	No asignado
5	Ámbito local de Sitio
6	No asignado
7	No asignado
8	Ámbito local de Organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ámbito Global
F	Reservado

Tabla. 2.5-5 Significados de los bit de ámbito

Autor: Investigador
Fuente: http://www.microsoft.com/latam/technet/articulos/200009/art07/default.asp

Existen direcciones multicast reservadas:

ff01::1 Todos los nodos

ff02::1 Todas las interfaces

ff01::2 Todos los routers locales

ff05::2 Todos los routers del sitio

La dirección ff02::1ffxx:xxxx se la llama solicited-node address y obliga a todos los nodos calcular su multicast en función de la unicast asociada. Para ello se sustituye los 24 bits de menor peso (los marcados con x) con la dirección original.

Por ejemplo la 3ffe:b00:c18:1fff::7f4 se convertirá en ff01::1:ff00:7f4 Ejemplos útiles de redes actualmente usadas:

- 3ffe::/16 red 6bone global
- 3ffe:ffff:/32 dirección especial 6bone de prueba
- 2002::/16 redes para direcciones túnel 6to49 globales

ANYCAST

Una dirección anycast se envía sólo a la interfaz que es la más “cercana” al origen, aunque identifica a varias interfaces, y normalmente a múltiples nodos. El tráfico de paquetes con direcciones Anycast se observa en la Figura 2.5-16

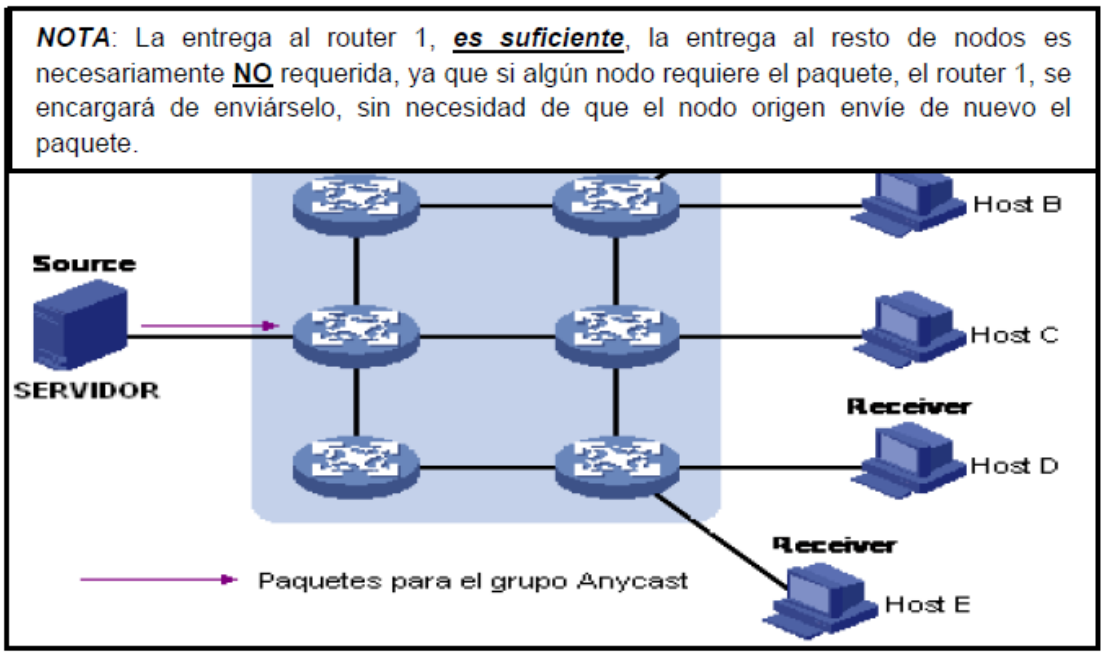


FIG.2.5-16 Direccionamiento Anycast IPv6

Autor: Investigador
Fuente: Ghislayae Xiomara Vera: Universidad de Loja-Zamora 2009

Tienen el mismo rango que las unicast, cuando una dirección unicast es asociada a más de una interfaz se convierte en una dirección anycast. Y existen direcciones asociadas a cada subred requeridas para los ruteadores (subnet router anycast address). Su formato es <prefijo de red><subred>::/n es decir el identificador de interfaz es el cero. Todos los paquetes que contengan esta dirección de destino serán enviados a dicha subred por los routers.

- fe80::/10 Asociada a toda interfaz local
- fec0::/10 Asociada a todo el sitio.

Por ejemplo

3ffe:b80:1daf:1::/64

- **3ffe:b80:1daf** es el identificador de la red freenet y **:1:** corresponde a la subred local. 1daf es el túnel asignado.

Representación de Dirección IPv6

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

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

A menudo una dirección posee alguna subcadena de varios ceros consecutivos de forma que se puede abreviar dicha cadena (sólo una vez, para evitar ambigüedades) mediante " : ". También se pueden omitir los ceros a la ceros a la izquierda dentro de un valor "x".

Los ceros a la izquierda de cada grupo se omiten, entonces :0001: puede simplificarse como :1: Por ejemplo a fe80::1 le corresponde con la forma canónica: fe80:0000:0000:0000:0000:0000:0000:0001.

Bloques contiguos de 16bits de ceros pueden simplificarse por única vez con ::, por ejemplo 2002:ffff:0:0:0:0:0:1 puede simplificarse como 2002:ffff::1 En la tabla 2.5.6 se puede ver los tipos de direcciones IPv6.

Dirección IPv6	Longitud del Prefijo (Bits)	Descripción	Notas
::	128 bits	sin especificar	como 0.0.0.0 en Pv4
::1	128 bits	dirección de bucle local (loopback)	como las 127.0.0.1 en IPv4
::00:xx:xx:xx:xx	96 bits	direcciones IPv6 compatibles con IPv4	Los 32 bits más bajos contienen una dirección IPv4. También se denominan direcciones "empotradas."
::ff:xx:xx:xx:xx	96 bits	direcciones IPv6 mapeadas a IPv4	Los 32 bits más bajos contienen una dirección IPv4. Se usan para representar direcciones IPv4 mediante direcciones IPv6.
fe80:: - feb::	10 bits	direcciones link-local	equivalentes a la dirección de loopback de IPv4
fec0:: - fef::	10 bits	direcciones site-local	Equivalentes al direccionamiento privado de IPv4
ff::	8 bits	multicast	
001 (base 2)	3 bits	direcciones unicast globales	Todas las direcciones IPv6 globales se asignan a partir de este espacio. Los primeros tres bits siempre son "001".

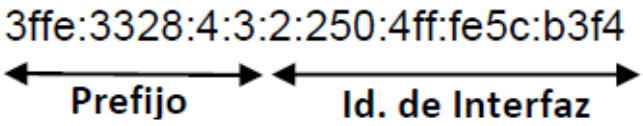
Tabla. 2.5-6 Tipo de Direccionamiento IPv6

Autor: Investigador
Fuente: http://www.arsys.es/ayuda/directorio/infraestructura-tecnica/ipv6.htm

Otra forma de escribir direcciones IPv6 es utilizando la ya tradicional notación decimal de IPv4 pero solamente para los 32 bits más bajos de la dirección IPv6. Por ejemplo a 2002::10.0.0.1 le correspondería con la representación hexadecimal canónica 2002:0000:0000:0000:0000:0000:0a00:0001 la cual es equivalente también a escribir 2002::a00:1.

La representación de direcciones IPv6 se realiza de tres formas:

- **Formato Preferido:**
  X:X:X:X:X:X:X:X (X = valores en hexadecimal de los ocho bloques de 16 bits de la dirección). Ejemplo:



- **Formato comprimido:**
  Este método permite agrupar largas series de 0's, para hacer más legibles las direcciones, el uso de "::" indica múltiples grupos de 16 bits a 0.
  Ejemplos:
  1080:0:0:0:8:800:200C:417A podría representarse como 1080::8:800:200C:417A
  FF01:0:0:0:0:0:0:43 podría representarse como FF01::43
  Sólo puede usarse "**::**" una vez en una dirección.

- **IPv4-compatible:**
  Este método resulta el más indicado para representar direcciones IPv6 que contengan direcciones IPv4, los 2 últimos bloques de 16 bits se representan como 4 bloques de 8 bits mostrando sus valores en decimal, como en IPv4.
  Ejemplos:
  0:0:0:0:0:0:13.1.68.3 ó ::13.1.68.3
  0:0:0:0:0:FFFF:129.144.52.38 ó ::FFFF:129.144.52.38.

Existen solo dos direcciones reservadas en ipv6:

- **Una es la dirección local ::1** (se están simplificando 31 ceros), esta solo se la puede asociar al dispositivo "loopback", es similar en ipv4 a la dirección privada 127.0.0.1.

- **Otra es :: (todo cero)** que corresponde a dirección no especificada y no puede usarse como dirección de nada. En cambio no existe la dirección broadcast, por lo tanto en teoría ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff es legítima, pero no se usa.

Otro concepto importante es el prefijo, este determina una reserva del espacio de direccionamiento de la dirección para definir la red, la sub-red, por ejemplo 2002::/**16** el prefijo es 16 y indica que los primeros 16 bits corresponden a la caracterización de la red.

2.5.4 SEGURIDAD DEL PROTOCOLO IPv6

William Jackson[17] publicó sobre la seguridad en IPv6, el protocolo base de comunicaciones que seguirá al actual IPv4.

Entre otras reflexiones, se habla sobre la posible madurez del protocolo para ser usado con IPSec, el problema que se supondrá para muchos dispositivos es el uso de cabeceras más largas y el impacto en la administración cotidiana de redes (el escaneo secuencial de rangos de red se volverá impracticable).

Tal y como se ha comentado en los puntos anteriores, debido al carácter científico que en un principio tuvo Internet, la seguridad no fue contemplada históricamente en ninguna de las capas que forman la estructura TCP/IP. Con el auge de las tecnologías de la información y el aumento de personas y empresas conectadas a Internet, la necesidad de seguridad se fue convirtiendo en uno de los aspectos más importantes. Además la proliferación de noticias sobre personas sin escrúpulos dedicadas a la piratería, creó un gran malestar social debido a la sensación de inseguridad por los ataques que sufrían tanto las empresas (bancos, universidades e incluso instituciones como la NASA) como los usuarios (utilización ilícita de números de tarjetas de crédito).

---

[17] **WILLIAN JACKSON:** Publicó sobre las seguridades de IPv6 que en la actualidad son utilizadas ciertos protocolos y otros cambiados.

Aprovechando la necesidad de adaptar los diferentes protocolos al crecimiento de Internet, se optó por introducir una serie de especificaciones para garantizar la seguridad como parte implícita de las nuevas especificaciones de los protocolos. Estas especificaciones se conocen como IP Security o IPSec.

Una vez que se había consensuado la necesidad de introducir especificaciones de seguridad como parte intrínseca de los protocolos y no como simples extensiones voluntarias para los fabricantes de software (como paso con la versión 5), se planteó un duro debate sobre que capa sería la idónea para proporcionar esta seguridad. Esta decisión era crítica, ya que en el mercado ya existían diferentes soluciones comerciales (SSL, SET) que proporcionaban distintos grados de seguridad en la capa de usuario.

Finalmente para evitar duplicidades y asegurar un sistema seguro y auténtico en todas las capas, se optó por incluir las especificaciones en el nivel más bajo de la pila (Stack) de protocolos, en la especificación del protocolo IP versión 6.

Internet Protocol Security (IPsec), el protocolo para cifrado y autenticación IP forma parte integral del protocolo base en IPv6. El soporte IPSec es obligatorio en IPv6 a diferencia de IPv4, donde es opcional (pero usualmente implementado).

Las seguridades de IPv6 se detallarán ampliamente con el protocolo IPSec en el siguiente Capítulo 3.

En este capítulo esta detallada la información a base de los diferentes RFC, las mismas que serán explicadas en los Anexos los tipos de RFC que fueron utilizados.

CAPITULO III

3. ESTRUCTURA DEL PROTOCOLO DE SEGURIDAD IPSec en IPv6

Una de las grandes ventajas de IPv6 es sin duda, la total integración de los mecanismos de seguridad, autentificación y confidencialidad (encriptación) dentro del núcleo del protocolo.

Se trata por tanto de algo obligatorio y no adicional como sucede en IPv4, de esta manera la cabecera puede tener valores AH (Autentificación, "Authentication Header") y ESP (Encriptación, "Encapsulation Security Payload"), que permiten básicamente, emplear las mismas extensiones de protocolo empleado en IPv4

La seguridad ha sido una pieza fundamental en IPv6 desde el comienzo de su estandarización, y dentro de esta funcionalidad se encuentra IPSec que genera sistemas de seguridad y será detallado en el siguiente punto.

IPSec puede ser empleado para proteger uno o más caminos entre:

- Pares de hosts
- Hosts y Gateway de seguridad
- Pares de Gateway de seguridad

De esta forma existen varios servicios que son importantes en IPv6 para las comunicaciones entre diferentes usuarios, Los servicios que IPSec puede proveer son:

- Control de Acceso
- Integridad no orientada a la conexión
- Autentificación de origen de datos
- Confidencialidad y Negociación de Compresión IP

Este capítulo proporciona una descripción de como trabaja IPSec, IKE, ISAKMP, con los componentes de seguridad que se detallarán en los siguientes puntos.

3.1 INTRODUCCION IPSEC

IPSec proporciona servicios de seguridad en la capa IP, permitiendo a un sistema seleccionar los protocolos de seguridad, determinar los algoritmos a utilizar para los servicios, e implementar cualquier algoritmo criptográfico requerido para proporcionar los servicios solicitados.

También se puede utilizar para proteger una o más trayectorias entre un par de hosts, o entre un par de security gateway, o entre ambos. El término security gateway se utiliza para referirse a un sistema intermedio que implementa los protocolos IPsec. Por ejemplo, un router o un firewall implementando IPsec es un security gateway.

Las especificaciones IPSec han sido definidas para trabajar en la capa inferior (Capa Fisica) de la pila (Stack) de protocolos TCP/IP, funcionando por lo tanto en el nivel de datagrama y siendo independientes del resto de protocolos de capas superiores (TCP, UDP).

Beneficios

Cuando se implementa IPSec en un router, éste provee una fuerte seguridad que puede ser aplicada a todo el tráfico que cruza por el router. Por otro lado, IPSec está debajo de la capa de transporte (TCP, UDP), así pues resulta transparente para las aplicaciones. No hay necesidad de cambiarlas, ni desde el punto de vista del usuario ni del servidor cuando IPSec se incorpora al router o al firewall.

También se tiene que IPSec puede ser transparente a los usuarios finales. Como una política general, puede asumirse que no es necesario involucrar a los usuarios en los mecanismos de seguridad. Finalmente, IPSec tiene la capacidad de ofrecer seguridad individual si ésta fuese indispensable. Tal característica es útil para empleados que accedan a la red desde el exterior, vía telefónica.

Además, es posible asegurar una subred virtual dentro de una organización para aplicaciones sensibles. En resumen, entre los beneficios de IPv6 importantes son:

- Herencia de niveles de seguridad, de routers a subredes.

- Transparencia respecto a las aplicaciones.
- Transparencia respecto a usuarios finales.
- Ofrecimiento de seguridad a nivel individual.

Como Trabaja IPSec

IPSec autentifica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre estaciones de trabajo y servidores, y entre servidores. El objetivo principal de IPSec es proporcionar protección a los paquetes IP. Está basado en un modelo de seguridad de extremo a extremo, lo que significa que los únicos hosts que tienen que conocer la protección de IPSec son el que envía y el que recibe.

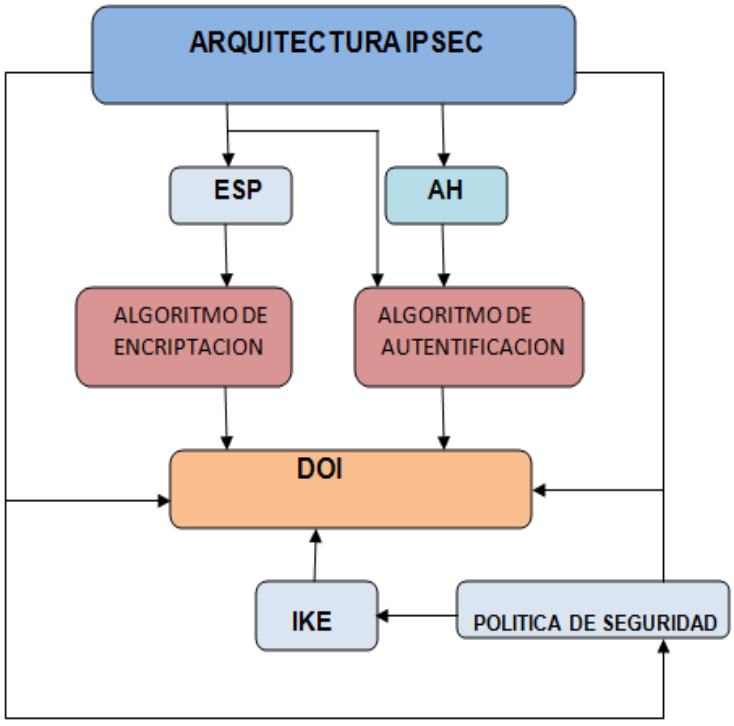


FIG.3.1-17 Arquitectura IPSEC

Autor: Investigador
Fuente: Universidad de México, Víctor Villagra; @2000, DIT-UPM

Cada equipo controla la seguridad por sí mismo en su extremo, bajo la hipótesis de que el medio por el que se establece la comunicación no es seguro, por esta razón IPSec ofrece las siguientes funcionalidades principales:

- Una asociación de seguridad (SA)
- Solo autenticación: Conocida como Authentication Header (AH)
- Cifrado + Autenticación: Conocida como Encapsulating Security Payload (ESP)
- Una función de gestión de Claves: IKE (ISAKMP)

La autenticidad y el cifrado de datos (o datagramas) requieren que tanto el emisor como el receptor compartan una clave, un algoritmo de cifrado/descifrado y una serie de parámetros (como el tiempo de validez de la clave) que diferencian una comunicación segura de otra. Estos parámetros conforman la asociación de seguridad (Security Association, SA) que permite unir la autenticidad y la seguridad en IPSec.

3.1.1 MODO DE FUNCIONAMIENTO DE IPSEC

También se debe tener en cuenta que IPSec se puede implementar en modo de transporte de host a host, así como en un modo de red de túneles, dependiendo del nivel sobre el que se actúe.

En modo transporte

En este modo transporte, pueden utilizarse el encabezado exterior, el encabezado siguiente y los puertos que admita el siguiente encabezado para determinar la directiva IPsec. con respecto a la cabecera IPv6, ver en el siguiente grafico (3.1-18)

Este modo sólo la carga útil del paquete IP es cifrada y / o autenticada. La ruta está intacta, ya que la cabecera IP no es ni modificada ni cifrada, sin embargo, cuando el encabezado de autenticación se utiliza, las direcciones IP no pueden

ser traducidas. El modo transporte se utiliza para las comunicaciones de host a host.

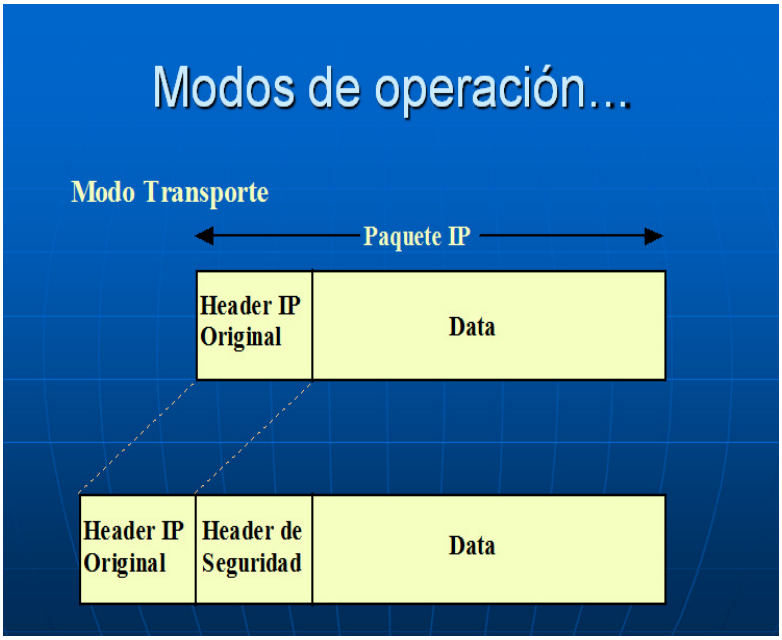


FIG.3.1-18 Modo Transporte de IPSec

Autor: Investigador
Fuente: Universidad de México, Víctor Villagra; @2000, DIT-UPM

En modo túnel

En el modo túnel todo el paquete IP (datos más cabeceras de mensajes) es cifrado y/o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. También se utiliza para comunicaciones red a red (túneles seguros entre routers para VPNs) o para comunicaciones de un host hacia la red (accesos de usuarios remotos) y una comunicación de host a host por medio de internet (charlas privadas)

Los protocolos son aplicados a paquetes (a los que se hizo un túnel a través de IP). Se realiza entre sistemas intermedios. Se establece un túnel seguro para encapsular los datagramas IP inseguros, ver en la figura (3.1-19).

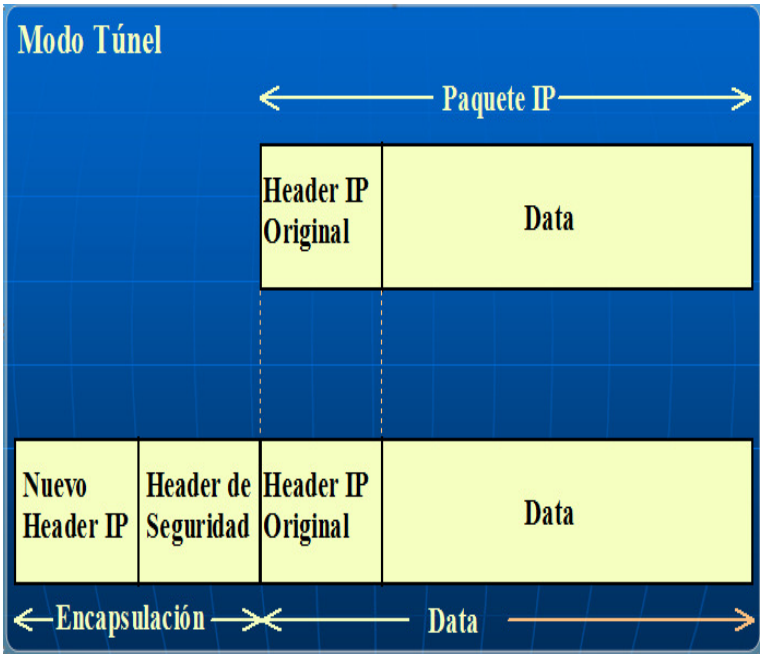


FIG.3.1-19 Modo Túnel de IPSec

Autor: Investigador
Fuente: Universidad de México, Víctor Villagra; @2000, DIT-UPM

3.2 COMPONENTES DE IPSEC

Los componentes de IPSec son los mecanismos principales para el funcionamiento de las seguridades en las comunicaciones, se debe detallar cada uno de estos componentes para conocer a profundidad el funcionamiento de estos protocolos que son en la actualidad la fase principal en las redes, para garantizar la seguridad de los mensajes y/o información. Los componentes fundamentales de IPSec se ampliaran en los siguientes puntos de este capítulo.

3.2.1 SECURITY ASSOCIATION (SA)

Asociación de Seguridad (Security Association (SA)) permite las especificaciones de los servicios de seguridad y los parámetros negociados en cada trayectoria segura IP, como los requisitos para administrar Asociaciones de Seguridad para

toda implementación IPv6 y para implementaciones IPv4 que implemente AH, ESP, o ambos. Las SAs se caracterizan por:

- El contexto de interoperabilidad usada en AH y ESP
- Relación uno a uno entre transmisor y receptor que define el conjunto de parámetros de seguridad utilizados
- Es necesario establecer una SA previamente a la comunicación: IKE

Lo que define una SA es:

- **Sequence Number Counter:** Valor de 32 bits para generar el número de secuencias transmitidos en las cabeceras AH y ESP.
- **Sequence Counter Overflow:** Indicador de acción ante un llenado del nº de secuencias.
- **Anti-Replay Window:** Ventana para limitar la aceptación de datagramas validos.
- **AH Information:** Algoritmos de autentificación, claves, tiempos de vida, usando AH.
- **ESP Information:** Algoritmo de cifrado y autentificación, claves, valores de inicio, tiempos de vida usando ESP.
- **IPSec Protocol Mode:** Modo de transporte o Túnel
- **SA Lifetime:** Intervalo de tiempo o bytes después del cual hay que sustituirla por una nueva SA.
- **Path MTU**: Máximo tamaño de paquetes transmitidos sin fragmentación.

En los siguiente punto 3.2.2 y 3.2.3 de este capítulo se detallará el Algoritmo de Autentificación (AH) y Algoritmo de Cifrado (ESP).

3.2.1.1 DEFINICION DE SA

Una Asociación de Seguridad (SA) es una conexión lógica unidireccional simplex que ofrece servicios de seguridad al tráfico transportado por este. Los servicios de seguridad ofrecidos en una SA son usados por AH o ESP, pero no por ambos. Si ambos (AH y ESP) se aplican a un flujo de tráfico, dos o más SAs se crearán para generar la protección de flujo del tráfico. Para asegurar la comunicación

bidireccional entre dos hosts, o entre dos puertas de enlace, se requieren dos Asociaciones de Seguridad (una en cada sentido).

Una SA es identificada únicamente por: un Índice de Parámetros de Seguridad (SPI), una dirección IP de destino, y un identificador de protocolo de seguridad (AH o ESP).

El Índice de Parámetros de Seguridad (SPI), se transmite en las cabeceras de AH y ESP para seleccionar la SA que procesará dicho mensaje, La dirección de destino puede ser una dirección unicast, una dirección de difusión IP, o una dirección de grupo multicast.

Sin embargo, los mecanismos IPsec para la gestión de SA se definen solamente para unicast. Aun cuando el concepto también es aplicable a conexiones punto a multipunto. El identificador de protocolos de seguridad permite identificar qué tipo de seguridad se usa en AH (solo autentificación) y ESP (cifrado y posiblemente autentificación).

SA se define en dos tipos: modo transporte y modo túnel.

SA en modo trasporte

Es una SA entre dos hosts. En IPv4 una cabecera de protocolo de seguridad en modo transporte aparece inmediatamente después de la cabecera IP y de algunas opciones, y antes que cualquier protocolo de capas superior (por ejemplo, TCP o UDP). En IPv6 las cabeceras del protocolo de seguridad se sitúan después de la cabecera IP y de extensiones pero deben aparecer antes o después de la cabecera de opciones de dirección y antes de los protocolos de capas superiores.

En el caso de ESP, una SA en modo transporte proporciona servicios de seguridad solamente para los protocolos de las capas superiores, no para la cabecera IP o cualquier cabecera de extensión precedente a la cabecera ESP.

En el caso de AH la protección se extiende a las partes seleccionadas de la cabecera IP, a las partes seleccionadas de las cabeceras de extensión y a las opciones seleccionadas. Ver la figura 3.2-20

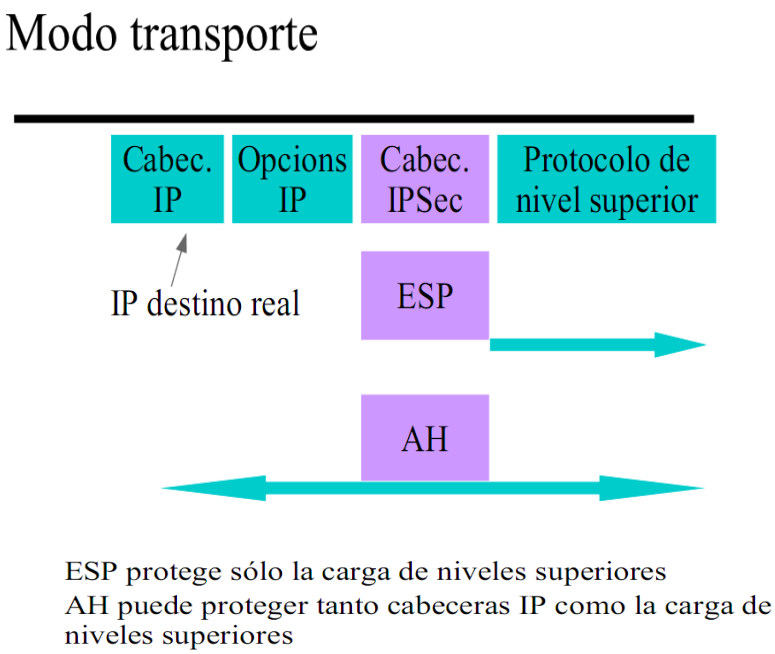


FIG.3.2-20 Modo Transporte SA

Autor: Investigador
Fuente: http://webdiis.unizar.es/~ftricas/Asignaturas/seguridadD/Transparencias/2-ConceptosBasicosSeguridadInformatica.pdf

SA en modo túnel

Es una SA aplicada a un túnel IP. Siempre que el final de una asociación sea una puerta de enlace segura, la SA debe estar en modo túnel.

Para una SA en modo túnel hay una cabecera IP "externa" que especifica el destinatario del proceso IPsec, más una cabecera IP "interna" que especifica el último destinatario aparentemente último del paquete.

La cabecera del protocolo de seguridad aparece después de otras cabeceras IP externas y antes de las cabeceras IP internas. Si se emplea AH en modo túnel, a otras partes de la cabecera IP se les ofrece protección así como también a todo el paquete IP al cual se le hizo el túnel (es decir, toda la cabecera IP interna es protegida, como así también protocolos de capas superiores). Si se emplea ESP, la protección es proporcionada únicamente al paquete IP al cual se le hizo el túnel (al paquete "tunelizado"), no a las cabeceras externas. Ver la figura 3.2-21

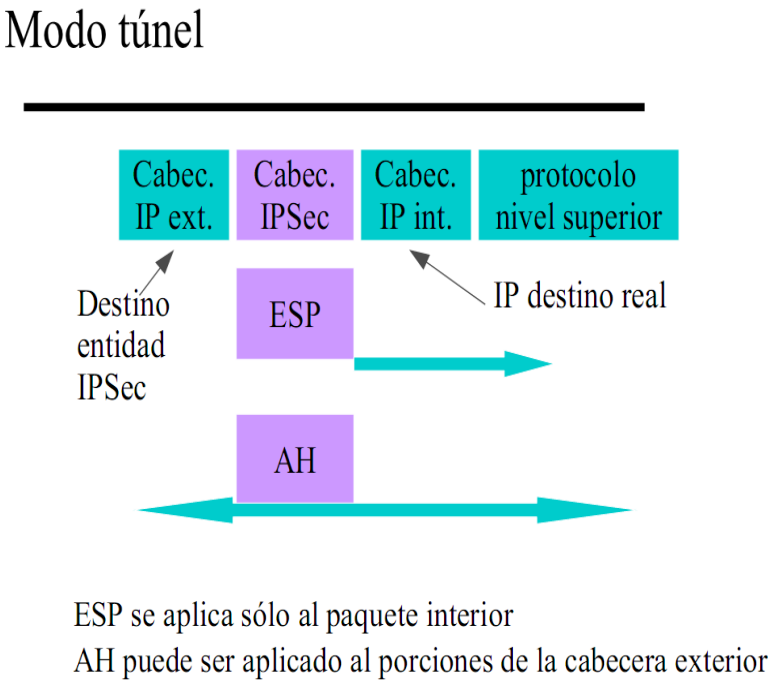


FIG.3.2-21 Modo Túnel SA

Autor: Investigador
Fuente: http://webdiis.unizar.es/~ftricas/Asignaturas/seguridadD/Transparencias/2-ConceptosBasicosSeguridadInformatica.pdf

3.2.1.2 MODO DE OPERACIÓN DEL SA

El conjunto de servicios de seguridad ofrecido por una SA depende del protocolo de seguridad seleccionado, del modo de la SA, de los extremos de la SA, y de la elección de los servicios opcionales seleccionados dentro del protocolo. Por ejemplo, AH proporciona autentificación del origen de los datos e integridad sin conexión para datagramas IP (a partir de ahora equivale a autentificación). La precisión de estos servicios de autentificación estará en función de la granularidad de la SA con la que se emplea AH.

AH ofrece además un servicio de anti-replay (integridad parcial de la secuencia) según el deseo del receptor, esto ayudará a prevenir ataques contra denegación de servicios. AH es un protocolo apropiado para emplearse cuando la confidencialidad no es requerida (o no se permite, por ejemplo, debido a las restricciones gubernamentales en el uso criptográfico). AH también proporciona

autentificación para las partes seleccionadas de la cabecera IP, que puede ser necesaria en algunos contextos. Por ejemplo, si la integridad de una opción de IPv4 o una cabecera de extensión de IPv6 se debe proteger en el camino entre el emisor y el receptor, AH puede proporcionar este servicio

ESP proporciona de forma opcional confidencialidad para el tráfico. (La robustez del servicio de confidencialidad depende en parte, del algoritmo de encriptación utilizado). ESP también proporciona de forma opcional, autenticación como en el caso anterior. Si la autentificación es negociada por una SA ESP, el receptor también puede elegir implementar el servicio de anti-replay con las mismas características que el servicio de anti-replay de AH.

La autentificación ofrecida por ESP abarca menos que la ofrecida por AH, es decir las cabeceras que quedan por fuera de la cabecera ESP no están protegidas. Si solo los protocolos de capas superiores necesitan ser autentificados, entonces la autentificación de ESP es una elección apropiada y es más eficiente en tamaño que usar ESP encapsulado con AH. Aunque la confidencialidad y la autenticación son opcionales en ESP, no se pueden omitir ambas, al menos una debe ser escogida.

Si se elige el servicio de confidencialidad, entonces una SA con ESP (en modo túnel). Entre dos puertas de enlace pueden ofrecer confidencialidad en un flujo de tráfico parcial. El uso del modo túnel permite encriptar las cabeceras IP internas, ocultando las identidades de la (última) vía de tráfico y el destino. También usar relleno en la carga de ESP para ocultar el tamaño de los paquetes.

3.2.1.3 COMBINACION DEL SA

Las combinaciones de SA deben ser completamente soportados por hosts IPsec o puertas de enlaces de seguridad. Combinaciones adicionales de AH y/o ESP en modo trasporte y/o túnel pueden ser soportadas a criterio del implementador.

La combinación básica dada en la SA se compone de cuatro casos que son necesarios:

- **CASO I**

Proporciona seguridad extremo a extremo entre 2 host a través de Internet (o una Intranet). Soporta modo transporte y modo túnel, en ambos hosts.

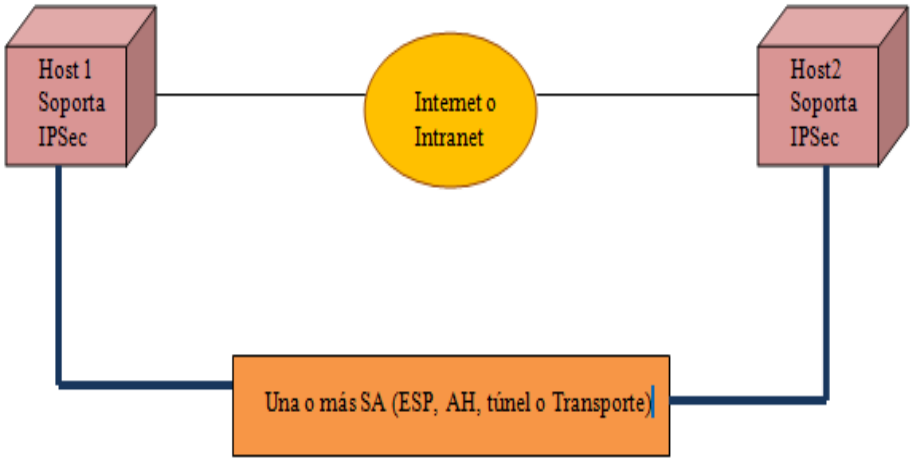


FIG.3.2-22 Combinación básica de SA (caso 1)

Autor: Investigador
Fuente http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

NOTA: Tanto el modo trasporte como el modo túnel pueden ser seleccionados en los host

En este caso no hay ninguna condición para el soporte de enrutamiento (de cabeceras), en modo trasporte, AH y ESP se pueden aplicar al paquete. En este caso, el procedimiento para establecer la SA se debe aplicar primero ESP, y luego aplicar AH al paquete

- **CASO II**

Este caso ilustra el soporte para una Red Privada Virtual simple VPN (Virtual Private Networks), solamente requiere modo túnel.

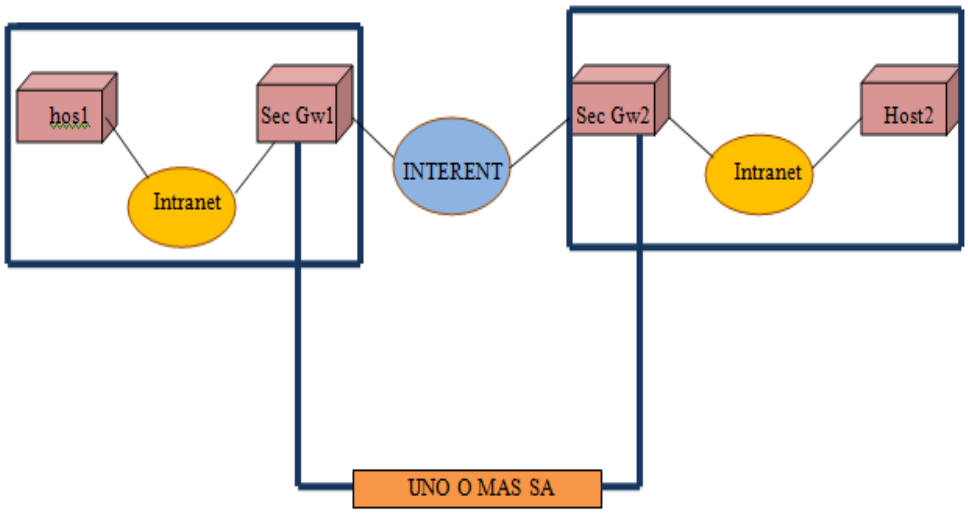


FIG.3.2-23 Combinación básica de SA (caso 2)

Autor: Investigador
Fuente http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

- **CASO III**

En este caso se combinan el caso 1 y el caso 2, agregando seguridad extremo a extremo entre el host emisor y el receptor. No impone ningún nuevo requisito en host, con excepción de que la puerta de enlace sea configurada para dejar pasar tráfico IPsec (incluyendo tráfico ISAKMP) a los host que están detrás de este.

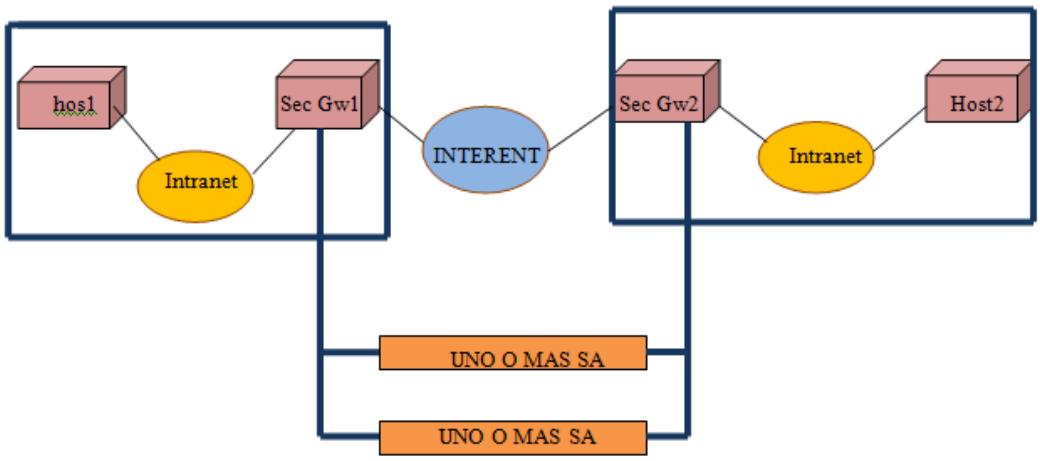


FIG.3.2-24 Combinación básica de SA (caso 3)

Autor: Investigador
Fuente http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

- **CASO IV**

En este caso un Host remoto utiliza Internet para alcanzar el firewall de una organización y entonces obtener acceso a un servidor en otra máquina. Se requiere el modo túnel entre el Host remoto y el firewall (caso 2). Las opciones para la SA entre los dos Hosts puede ser cualquiera de las del caso 1.

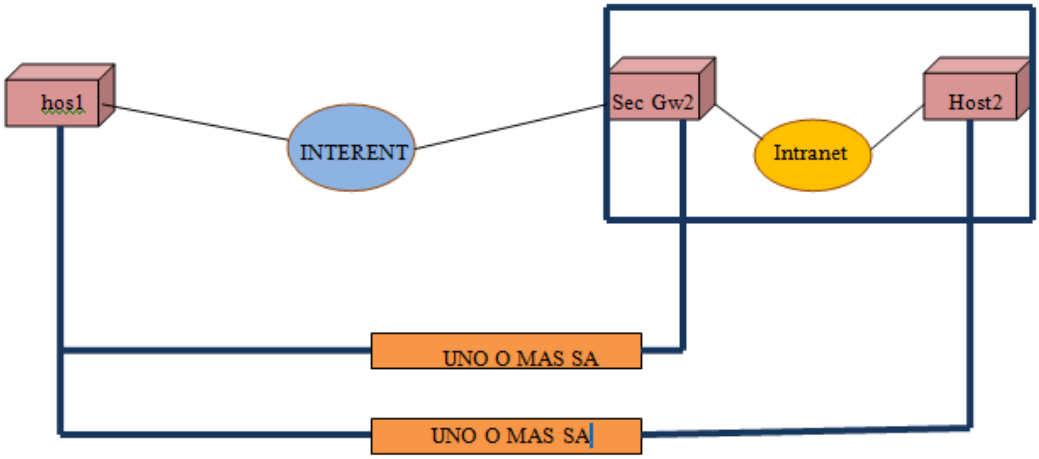


FIG.3.2-25 Combinación básica de SA (caso 4)

Autor: Investigador
Fuente http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

3.2.1.4 BASE DE DATOS SA

En IPSec hay dos bases de datos que detallan el procesamiento del tráfico. La base de datos de política de seguridad (SPD) y la base de datos de asociación de seguridad (SAD). Estas dos bases se detallarán más ampliamente en el punto 3.2.1.4.1 de este capitulo

La primera especifica las políticas que determinan el tratamiento de todo el tráfico IP de entrada o salida de un Host y puerta de enlace segura. La segunda contiene los parámetros asociados a cada SA. También se define un selector, que es un conjunto de campos con valores del protocolo IP y capas superiores que son usados por la SPD para mapear el tráfico con una política por ejemplo una SA.

3.2.1.4.1 BASE DE DATOS DE POLITICAS DE SEGURIDAD (SPD)

Una SA es generada por la gestión usada para implementar una política de seguridad en el ambiente IPsec. De esta manera un elemento esencial del proceso de la SA es una SPD subyacente que especifica qué servicios deben ser ofrecidos a los datagramas IP y de qué forma. La forma de la base de datos y su interfaz no se especifican.

Para cada implementación IPSec debe haber una interfaz de administración que permita al administrador del sistema manejar la SPD. Los paquetes de entrada y salida son propensos a ser tratados por IPSec y la SPD debe especificar que acción ha de realizar en cada caso.

Una SPD debe diferenciar entre el tráfico al que debe ofrecer protección IPsec de al que le está permitido evitar IPsec. Esto implica que la protección IPsec a ser empleada debe estar presente tanto en el receptor como en el emisor. Para cualquier datagrama de entrada o de salida, hay tres opciones de procesamiento posibles:

- **Descartar:** es el tráfico al que no se permite salir del host, atravesar una puerta de enlace, o que se entregue a una aplicación.

- **Evitar IPsec (no IPsec):** se refiere al tráfico que se le permite pasar sin la protección de IPsec.

- **Que se aplique IPsec:** es el tráfico que es protección producida por IPsec, y para tal tráfico la SPD debe especificar los servicios de seguridad que se proporcionarán, los protocolos que se emplearán, los algoritmos que se utilizarán.

Específicamente, cada paquete de entrada o de salida está sujeto al procesamiento IPsec, y la SPD deberá especificar qué acción será tomada en cada caso. La interfaz administrativa debe permitir que el usuario (o el administrador del sistema) especifique que proceso de seguridad ha de ser aplicado a cada paquete entrante o saliente del sistema. La interfaz de gestión para el SPD debe permitir la creación de entradas consistentes con los selectores

y debe soportar el ordenamiento total de esas entradas. Los selectores son análogos a los que se encuentran en un firewall.

En un sistema host, las aplicaciones se pueden permitir seleccionar que proceso de seguridad debe ser aplicado al tráfico que generan y consumen. El administrador del sistema debe poder especificar si una aplicación puede o no reemplazar la política del sistema.

El SPD contiene una lista ordenada de políticas de entrada. Cada política de entrada es introducida por uno o más selectores que definen el conjunto de tráfico IP comprendido por esta política de entrada. Estos definen la granularidad de las políticas o SAs. Cada entrada incluye un indicador para el tráfico coincidente con esta política, si será desviado, desechado, o procesado por IPsec.

Si el procesamiento IPsec es aplicado, la entrada incluirá una especificación de SA (o grupo de SA), como son el listado de Protocolos IPsec, los modos, y algoritmos que se emplearán e incluirán cualquier requisito relacionado. La SPD se utiliza para controlar todo el flujo de tráfico en IPsec incluyendo seguridad, manejo de claves (por ejemplo ISAKMP), tráfico entrante y saliente de entidades detrás de una puerta de enlace. Esto significa que el tráfico ISAKMP se debe referenciar explícitamente en la SPD, sino será descartado.

3.2.1.4.2 BASE DE DATOS DE ASOCIACION DE SEGURIDAD (SAD)

Cada SA tiene una entrada en la SAD y cada entrada define los parámetros asociados a esa SA. Para el procesamiento de entrada, cada entrada en la SAD es indexada por una dirección IP de destino el tipo de protocolo IPsec y SPI. Para el procesamiento de entrada los siguientes campos del paquete se usan para buscar la SA en la SAD y son requeridos para toda implementación:

- Dirección IP de Destino: otras cabeceras: La dirección de destino IPv4 o IPv6.
- Protocolo IPsec: AH o ESP: usado como un índice para buscar la SA en esta base de datos. Especifica el protocolo IPsec aplicado al tráfico en esta SA

- SPI: es un valor de 32 bits que se usa para diferenciar SAs diferentes que tienen el mismo destino (la misma dirección IP de destino) y que usan el mismo protocolo IPsec.

Para cada uno de los selectores definidos, la entrada de la SA en la SAD debe contener el valor o los valores que fueron negociados para esa SA cuando fue creada.

Para el emisor, estos valores se utilizan para decidir si una SA dada es apropiada para usarse con un paquete de salida. Esto es parte de la comprobación para saber si una SA existente puede ser utilizada. Para el receptor, este valor es utilizado para comprobar que los valores de los selectores en un paquete de entrada concuerdan con aquellos para la SA. Para el receptor esta es parte de la verificación de que la SA fue la correcta para el paquete.

Los siguientes campos de la SAD son usados en el procesamiento IPsec:

- **Contador de número de secuencia:**

  Un valor de 32 bit usado para generar el campo Número de Secuencia de la cabecera AH o ESP. Requerido por toda implementación, pero es usado solamente por el tráfico saliente

- **Desbordamiento del contador de secuencia:** Una bandera (flag) que indica si el desbordamiento del Contador del Número de Secuencia debería generar un acontecimiento auditable y prevenir la transmisión de los paquetes adicionales en la SA. Esto es requerido por toda implementación, pero es usado solamente para el tráfico saliente

- **Ventana anti-replay:** Un contador de 32 bits y un asignador de bits (bit-map) usado para determinar si un paquete AH o ESP es un paquete duplicado. Este debe ser requerido por toda implementación, pero es usado solamente para el tráfico entrante.

- **Algoritmo de autentificación AH, claves:** Este es requerido esencialmente por la implementación AH

- **Algoritmo de encriptación ESP, claves:** Este es requerido esencialmente por la implementación ESP

- **Algoritmo de autentificación ESP:** Si el servicio no se selecciona este campo será nulo debe ser requerido por la implementaciones ESP

- **Tiempo de vida de la SA:** Un intervalo de tiempo después del cual una SA debe ser reemplazada por una nueva SA

3.2.1.5 GESTION DE CLAVES DE SA

La gestión de claves permite a IPsec dar soporte para SA tanto manuales como automatizadas y la gestión criptográfica de claves. El protocolo IPsec, AH y ESP son en gran medida independientes de las técnicas de gestión asociadas a las SA, aunque las técnicas empleadas afectan un poco el servicio de seguridad ofrecido por los protocolos. Por otra parte la variedad empleada para la distribución de claves con IPsec determinará la autentificación proporcionada.

En general la autentificación del origen de los datos en AH y ESP está limitada por el alcance en el uso del secreto del algoritmo de autentificación que se comparten entre las múltiples fuentes posibles.

Gestión Manual

La forma más simple de gestión es administrando en forma manual, en la cual una persona configura manualmente, cada sistema con material clave y administra los datos de las SA relevantes a las comunicaciones seguras con otros sistemas.

Las técnicas manuales se usan en ambientes estáticos pequeños, pero la escalabilidad es mala. Por ejemplo una compañía puede crear una VPN usando IPsec en una puerta de enlace en varios sitos. Si el número de sitios es pequeño y como todos los sitios están bajo el mismo dominio administrativo, este es un contexto factible para las técnicas administrativas manuales. En este caso la puerta de enlace puede proteger selectivamente el tráfico y desde otros sitios dentro de la organización usando una configuración manual de claves, mientras que no proteja tráfico para otros destinos. También puede ser apropiado cuando solo se selecciona comunicaciones que necesitan ser seguras.

Gestión Automatizada

Este tipo de gestión es requerido para facilitar el uso de las características anti-replay de AH y ESP y para una adecuada creación de SA bajo demanda, por ejemplo, para el uso de claves orientadas a usuarios o a sesiones.

El protocolo de gestión de claves automáticas por defecto que usa IPsec es IKE bajo el Domino de Interpretación (DOI) de IPsec, a través de ISAKMP. Se pueden emplear otros protocolos para el manejo automatizado de SA. Cuando los protocolos de gestión de claves/SA se emplean, la salida de estos protocolos pueden ser empleados para crear múltiples claves.

El Sistema de Gestión de Claves puede proporcionar una cadena separada de bits para cada clave o puede generar una cadena de bits de la cual se extraigan todas las claves. Si una sola cadena de bits es proporcionada, hay que tener en cuenta que las partes del sistema que asignen la cadena de bit a las claves requeridas lo hagan en la misma forma en ambos extremos de la SA.

Para garantizar que las implementaciones IPsec en cada extremo de la SA usan los mismos bits para las mismas claves, independientemente de que parte del sistema divide la cadena de bits entre las claves individuales, la clave o claves encriptadas deben ser extraídas de los primeros bits (los de más a la izquierda, de orden superior) y la clave de autentificación debe ser tomada de los bits restantes.

3.2.1.6 PROCESAMIENTO DE ICMP

ICMP es el Protocolo de Mensajes de Control de Internet o es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando por ejemplo que un servicio determinado no está disponible o que un router o host no puede ser localizado.

Los mensajes ICMP son comúnmente generados en respuesta a errores en los datagramas de IP o para diagnóstico y ruteo. La versión de ICMP para IPv4 también es conocida como ICMPv4. IPv6 tiene su protocolo equivalente ICMPv6.

Los mensajes ICMP son construidos en el nivel de capa de red. IP encapsula el mensaje ICMP apropiado con una nueva cabecera IP (para obtener los mensajes de respuesta desde el host original que envía), y transmite el datagrama resultante de manera habitual.

Por ejemplo, cada router que reenvía un datagrama IP tiene que disminuir el campo de tiempo de vida (TTL) de la cabecera IP en una unidad; si el TTL llega a 0, un mensaje ICMP "Tiempo de Vida se ha excedido en transmitirse" es enviado a la fuente del datagrama.

La utilidad del protocolo ICMP es controlar si un paquete no puede alcanzar su destino, si su vida ha expirado, es decir, se usa para manejar mensajes de error y de control necesarios para los sistemas de la red, informando con ellos a la fuente original para que evite o corrija el problema detectado.

Hay dos aplicaciones simples y muy extendidas basadas en ICMP:

- El Ping: usa los mensajes ICMP Echo y Echo Reply para determinar si un host es alcanzable.
- El Traceroute: envía datagramas IP con bajos TTLs para que expiren durante la ruta que les dirige al destino. Utiliza los valores de los mensajes ICMP Time Exceded para determinar en qué parte de la red expiraron los datagramas y reconstruye así un esquema de la ruta hasta el host de destino.

Este protocolo se define dentro de IPv4 e IPv6 para la detección de errores de los mensajes.

ICMP para IPv6

ICMPv6 es un protocolo de propósito múltiple y está diseñado para realizar funciones tales como detectar errores encontrados en la interpretación de paquetes, realizar diagnósticos, funciones como Neighbor Discovery y detectar direcciones IPv6 multicast. Por esta razón, los mensajes ICMPv6 están subdivididos en dos clases: mensajes de error y mensajes informativos. Los mensajes ICMPv6 son enviados dentro de paquetes IPv6 los cuales a su vez pueden llevar las extensiones de cabecera de IPv6, y se caracterizan:

- ICMP para IPv6 usará un nuevo número de protocolo para distinguirlo de ICMPv4.
- El formato de la cabecera ICMP permanecerá igual.
- Las longitudes de los campos de los mensajes cambiarán para ajustarse a los mensajes IPv6, que serán de mayor longitud.
- El tamaño de los mensajes ICMP aumentará con el fin de explotar el tamaño máximo aumentado de los paquetes que IPv6 puede trasmitir sin fragmentar.
- La variante Fragmentation Required del mensaje ICMP Destination unreachable será reemplazado por el mensaje "Packet Too Big" que incluirá la MTU (Maximum Transmission Unit) de salida en la que se ha localizado el problema. Et tipo de característica se detallará en Mensajes de error de ICMP

Regla de los mensajes de ICMP para IPv6

Un nodo que reenvía un mensaje ICMPv6, debe determinar tanto la dirección IPv6 origen como la destino para el mensaje ICMPv6. Si un nodo tiene más de una dirección unicast, debe elegir la dirección origen del mensaje de la siguiente forma:

- Si el mensaje es una respuesta a un mensaje enviado a una de la direcciones unicast del nodo, la dirección origen de la respuesta debe ser esa misma dirección.

- Si el mensaje es una respuesta a un mensaje enviado a un grupo multicast o anycast al cual el nodo pertenece, la dirección origen de la respuesta debe ser una dirección unicast perteneciente a la interfaz en la cual el paquete multicast o anycast fue recibido.

- Si el mensaje es una respuesta a un mensaje enviado a una dirección que no pertenece al nodo, la dirección origen de la respuesta debe servir para comprobar el error (por ejemplo, la dirección unicast perteneciente a la interfaz en la cual el reenviado del paquete falló).

- En otros casos, se deben examinar las tablas de enrutamiento del nodo para determinar que interfaz debe ser usada para transmitir el mensaje a su destinatario, y la dirección unicast perteneciente a esa interfaz debe ser usada como dirección origen del mensaje.

Cuando un nodo ICMPv6 recibe un paquete, debe realizar acciones en función del tipo de mensaje. El protocolo ICMPv6 debe limitar el número de mensajes de error enviados a un mismo destinatario para evitar sobrecarga en la red.

Mensajes de error protegidos por ESP o AH

Un mensaje de error ICMP protegido por ESP o AH y generado por un router debe ser procesado y enviado por una SA en modo túnel. La política local determina si está o no subordinado a la comprobación de la dirección de origen por el router en el extremo destinatario del túnel.

Si el router en el extremo iniciador del túnel esta reenviando un mensaje de error ICMP para otro router, la comprobación de la dirección de origen podría fallar. Un mensaje ICMP protegido por AH o ESP y generado por un router no debe ser enviado en una SA en modo trasporte (a menos que la SA haya sido establecida

para el router actuando como un host, por ejemplo una conexión telnet usada para gestionar un router).

Un mensaje ICMP generado por un host debe realizar comprobaciones entre los selectores de direcciones IP de origen vinculados a la SA dentro de la cual el mensaje llega. Si el origen de un mensaje ICMP de error sea autentificado, la cabecera IP reenviada esta podría no ser válida. Por lo cual los valores del selector en la cabecera IP deben ser comprobados para asegurar que son consistentes con los selectores de la SA por la cual el mensaje ICMP fue recibido.

3.2.1.7 PROCESAMIENTO DE MTU

El MTU (Maximum Transmission Unit / Unidad máxima de transferencia) es un parámetro que indica el tamaño máximo que debe tener un datagrama para que sea transmitido por una interfaz IP sin que necesite ser fragmentado en unidades más pequeñas. El MTU debe ser superior al datagrama más grande que se desea transmitir para que no sea fragmentado. Lo que permite, el MTU expresa el tamaño máximo (en bytes) de un paquete que puede ser transmitido de una sola vez. Algunos valores del MTU:

- Ethernet: 1518 bytes.
- PPPoE: 1492 bytes
- RTC: 576 bytes
- ATM: 8190 bytes
- FDDI: 4470 bytes

Para el caso de IP, el máximo valor de la MTU es 65.536 bytes. Sin embargo, ése es un valor máximo teórico, pues, en la práctica, la entidad IP determinará el máximo tamaño de los datagramas IP en función de la tecnología de red por la que vaya a ser enviado el datagrama.

Por defecto, el tamaño de datagrama IP es de 576 bytes. Sólo pueden enviarse datagramas más grandes si se tiene conocimiento de que la red destinataria del datagrama puede aceptar ese tamaño. En la práctica, dado que la mayoría de

máquinas están conectadas a redes Ethernet o derivados, el tamaño de datagrama que se envía es con frecuencia de 1500 bytes.

Los datagramas pueden pasar por varios tipos de redes con diferentes tamaños aceptables antes de llegar a su destino. Por tanto, para que un datagrama llegue sin fragmentación al destino, debe ser menor o igual que el mínimo MTU de las redes por las que pase.

Para encontrar el MTU, se debe acceder a la línea de comandos (Inicio /Ejecutar / escribir cmd). Una vez en la línea de comandos, se realiza las pruebas de ping, precisando el tamaño de los paquetes que se va a probar: ping -f -l (tamaño del paquete -28) (IP del servidor) la opción -f permite hacer la prueba obligando a los routers encontrados a no fragmentar el paquete la opción –l envía el tamaño del paquete.

Resta 28 al tamaño del paquete que va a probar, correspondiente a la cabecera de este paquete

3.2.2 CABECERA DE AUTENTIFICACION (AH)

El protocolo AH es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los datagramas IP. Proporciona un medio al receptor de los paquetes IP para autenticar el origen de los datos y para verificar que dichos datos no han sido alterados en tránsito. Sin embargo no proporciona ninguna garantía de confidencialidad, es decir, los datos transmitidos pueden ser vistos por terceros.

Tal como indica su nombre, AH es una cabecera de autenticación que se inserta entre la cabecera IP estándar (tanto IPv4 como IPv6) y los datos transportados, que pueden ser un mensaje TCP, UDP o ICMP, o incluso un datagrama IP completo.

3.2.2.1 FUNCIONAMIENTO DE LA CABECERA DE AUTENTIFICACION

La Cabecera de Autentificación (AH) se usa para proporcionar integridad sin conexión y autenticación del origen de datos para datagramas IP y para proporcionar protección contra reenvíos.

AH proporciona autentificación a las partes de la cabecera IP que se les pueda brindar este servicio, así como también a los datos de los protocolos de las capas superiores. Sin embargo, algunos campos de la cabecera IP pueden cambiar durante el transporte, y el valor de estos campos, cuando el paquete llega al receptor, puede que no sea previsible para el emisor. Los valores de tales campos no pueden ser protegidos por AH. Así la protección proporcionada a la cabecera IP por AH se proporciona solo a partes de la cabecera IP.

AH se puede aplicar solo, o en combinación con la Carga de Seguridad Encapsulada (ESP), o a través de la modalidad anidada usando el modo túnel. Los servicios de seguridad pueden ser suministrados a comunicaciones, entre un par de hosts, o entre un par de puerta de enlace o entre una puerta de enlace y un host. ESP puede ser usado para proporcionar los mismos servicios de seguridad, y también para proporcionar un servicio de confidencialidad (encriptación). La diferencia principal entre la autentificación proporcionada por ESP y la de AH es la extensión de la cobertura.

Específicamente, ESP no protege ninguno de los campos de la cabecera IP a menos que esos campos sean encapsulados por ESP (en modo túnel).

El protocolo AH protege la integridad del datagrama IP. Para conseguirlo, el protocolo AH calcula una HMAC basada en la clave secreta, el contenido del paquete y las partes inmutables de la cabecera IP (como son las direcciones IP). Tras esto, añade la cabecera AH al paquete.

El algoritmo HMAC se detallará más delante de este capítulo.

En la siguiente figura 3.2-26 se muestra como funciona la cabecera de autentificacion

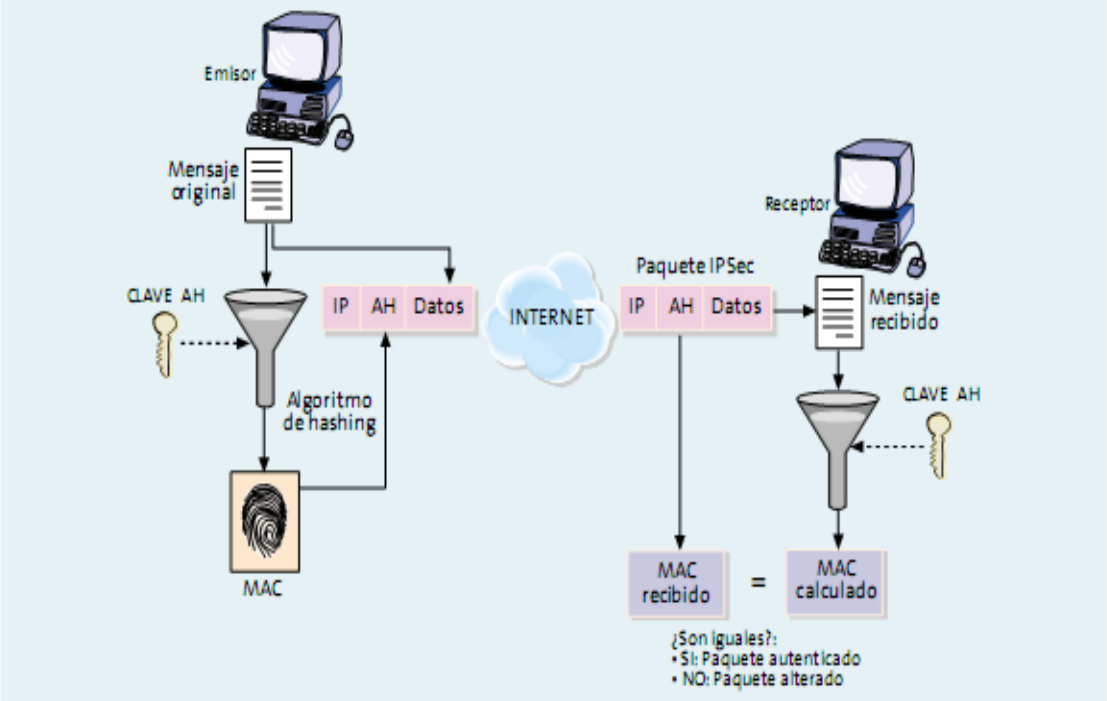


FIG.3.2-26 Funcionamiento de la Cabecera de Autentificación

Autor: Investigador
Fuente: http://www.telefonica.es/on/io/es/atencion/tutoriales_articulos/pdf/IPSec.pdf

La función de AH se basa en un algoritmo HMAC, esto es un código de autentificación de mensajes. Este algoritmo consiste en aplicar una función hash a la combinación de uno datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que se denomina extracto.

Dicho extracto tiene la propiedad de que es como una huella personal asociada a los datos y a la persona que lo ha generado, puesto que es la única que conoce la clave. En la figura se muestra todo el funcionamiento de AH donde el emisor calcula un extremo del mensaje original, el cual se copia de uno de los campos de la cabecea AH.

El paquete así construido se envía a través de la red, repitiéndole en el extremo receptor al cálculo del extremo y comparándole con el recibido en el paquete.

Si son iguales el receptor tiene la seguridad de que el paquete IP no ha sido modificado en el transito y que procede del origen esperado.

Si se analiza con detalle el protocolo AH, se puede concluir que su seguridad reside en que el cálculo del extracto (MAC) es imposible sin conocer la clave, y que dicha clave solo la conoce el emisor y el receptor.

3.2.2.2 ESTRUCTURA DE LA CABECERA DE AUTENTIFICACION

AH asegura la integridad de los datos mediante la suma de comprobación que genera un código de autenticación de mensajes, como por ejemplo MD5. Para asegurar la autenticación del origen de los datos, AH incluye una clave compartida secreta en el algoritmo que utiliza para la autenticación. Para asegurar la protección contra la reproducción, AH utiliza un campo de números de secuencia dentro de la cabecera AH.

Es importante observar que, a menudo, estas tres funciones distintas se concentran y se conocen como autenticación. En términos más sencillos, AH asegura que no se han manipulado los datos mientras se dirigían a su destino final.

La estructura de la cabecera de autentificación se basa de varios campos que pueden ser empleados en IPv4 e IPv6. Estos campos cumplen una función específica dentro de esta cabecera. Ver la figura 3.2-27

El algoritmo MD5 se detallará más delante de este capítulo.

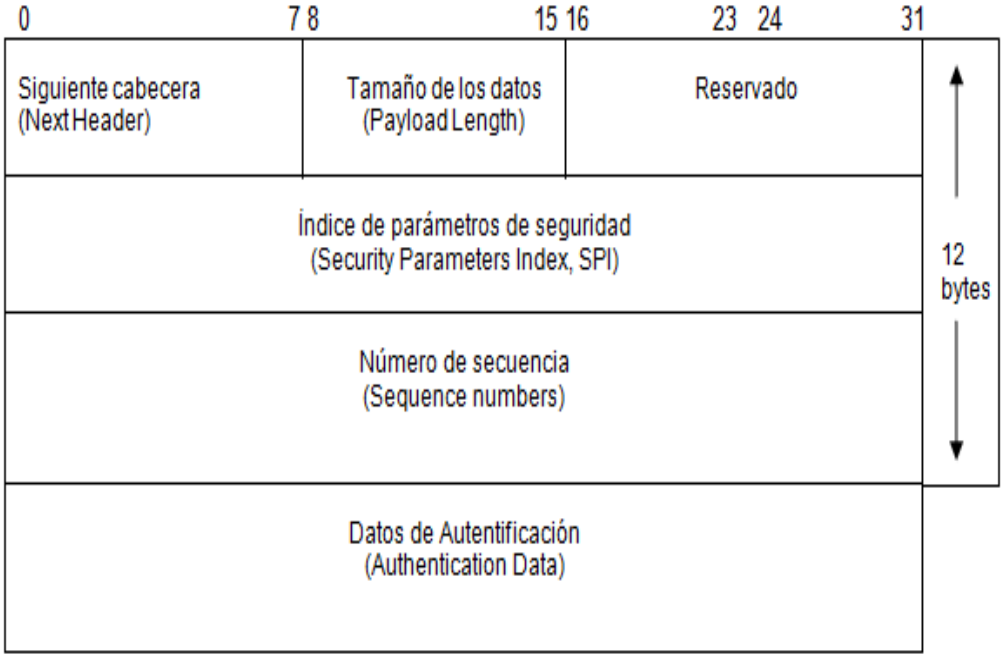


FIG.3.2-27 Estructura de la Cabecera de Autentificación

Autor: Investigador
Fuente http://es.wikipedia.org/wiki/IPsec

Campo Cabecera Siguiente

Es un campo de 8 bits que identifica el tipo de carga siguiente después de la Cabecera de Autentificación. Identifica cuál es el siguiente protocolo es decir cuál es el protocolo que será autentificado, cuál es el payload.

Campo Tamaño de los Datos

Este campo de 8 bits especifica la longitud de AH en palabras de 32 bit (en unidades de 4 bytes).

Campo Reservado

Este permite reservar para futuras aplicaciones. Debe estar a 0, ya que este campo es de 16 bits Se debe tener en cuenta que este valor está incluido en el cálculo de los datos de autentificación, pero es ignorado por el receptor.

Campo Índice de Parámetros de Seguridad SPI

Indica los parámetros de seguridad que, en combinación con la dirección IP, identifican la asociación de seguridad implementada con este paquete.

El SPI es un valor arbitrario de 32 bits que, conjuntamente con la dirección de destino IP y el protocolo de seguridad (AH), identifican a la Asociación de Seguridad para este datagrama. El conjunto de valores de SPI en el rango de 1 a 255 están reservados por la IANA para uso futuro.

La necesidad del SPI se hace evidente cuando se tiene más de una comunicación con la misma dirección IP de destino y protocolo de seguridad (AH o ESP). En teoría entonces, se puede tener (2^32) Asociaciones de Segundad con la misma dirección IP de destino y protocolo de seguridad.

Campo Número de Secuencia

Es utilizado para evitar ataques de repetición. Identifica en número del datagrama en la comunicación, estableciendo un orden y evitando problemas de entrega de datagramas fuera de orden o ataques externos mediante la reutilización (Replay Attacks) de datagramas.

Campo Datos de Autentificación

Se obtienen realizando operaciones (depende del algoritmo de cifrar escogido) entre algunos campos de la cabecera IP, la clave secreta que comparten emisor y receptor y los datos enviados. Este campo debe contener un múltiplo entero de 32 bits de longitud

3.2.2.3 LOCALIZACION DE LA CABECERA DE AUTENTIFICACION

La localización de AH se puede hacer de dos formas: Modo de Transporte y Modo Túnel.

Modo de Transporte AH

En la modalidad de transporte, la cabecera IP del datagrama se encuentra en la parte más externa de la cabecera IP, seguida de la cabecera AH y, a continuación, la carga útil del datagrama. AH autentica el datagrama entero, a excepción de los campos mutables. Sin embargo, la información que contiene el datagrama se transporta como texto legible y, por lo tanto, está sujeto a lecturas. La modalidad de transporte necesita menos actividad general del proceso que la modalidad de túnel, pero no proporciona tanta seguridad.

Este tipo de modalidad permite proteger el intercambio de información entre dos usuarios finales. La protección puede ser autentificación o encriptación (o las dos), pero no se hace usando un túnel.

En modo trasporte, AH se inserta después de la cabecera IP y antes del protocolo de capa superior, por ejemplo, TCP, UDP, ICMP o antes de cualquier otra cabecera IPsec que ya se haya incluido.

En el contexto IPv6, el AH se ve como carga extremo a extremo (end-to-end), y debe aparecer después de las cabeceras de extensión: salto-por-salto (hop-by-hop), de encaminamiento (routing), y de fragmentación. Las cabeceras de extensión opciones de destino podrían aparecer antes o después de la cabecera AH dependiendo de la semántica deseada. El diagrama siguiente ilustra AH en modo trasporte colocado en un paquete típico de IPv6.

Ver en la figura 3.2-28 El ingreso de AH en IPv4 e IPv6

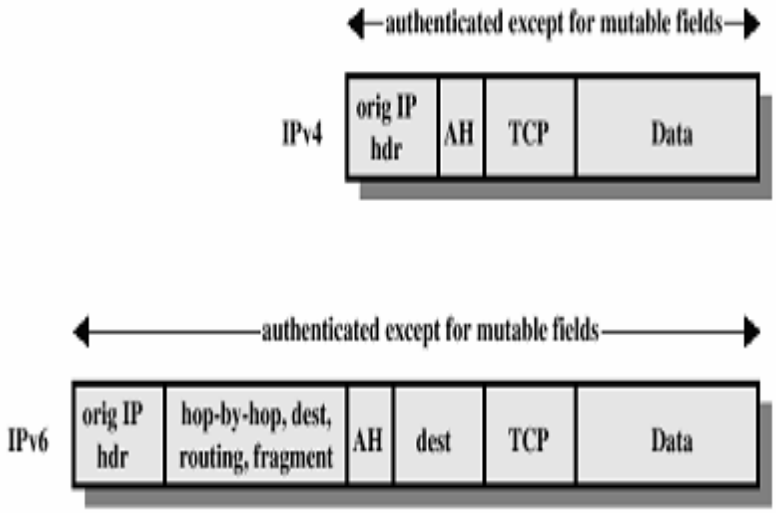


FIG.3.2-28 Modo Transporte de AH

Autor: Investigador
Fuente http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

Modo Túnel

La modalidad de túnel crea una nueva cabecera IP y la utiliza como parte más externa de la cabecera IP del datagrama. La cabecera AH continúa en la nueva cabecera IP. El datagrama original (tanto la cabecera IP como la carga útil original) aparece en último lugar. AH autentica el datagrama entero, por lo tanto, el sistema que responde puede detectar si el datagrama ha cambiado por el camino.

En la modalidad de túnel, las direcciones de origen y destino de la parte más externa de la cabecera IP no tienen necesariamente que ser iguales que las direcciones de la cabecera IP original. Por ejemplo, dos pasarelas de seguridad pueden operar un túnel AH para autenticar todo el tráfico entre las redes que conectan. De hecho, esta es una configuración muy habitual.

La principal ventaja de utilizar esta modalidad de túnel es proteger totalmente el datagrama IP encapsulado. Además, la modalidad de túnel hace posible utilizar direcciones privadas.

Este tipo de modalidad se puede utilizar en hosts y en puertas de enlace seguras. Si se emplea en puertas de enlace se tiene que usar el modo túnel. En éste modo la cabecera interna posee el origen y destino finales, mientras que la cabecera interna posee direcciones distintas (las puertas de enlace). La cabecera AH protege a toda la cabecera interna, incluida la totalidad de la Cabecera IP interna. La posición de la AH respecto a la cabecera IP externa es la misma que en el modo transferencia.

Ver en la figura 3.2-29 El ingreso en modo túnel de AH en IPv4 e IPv6.

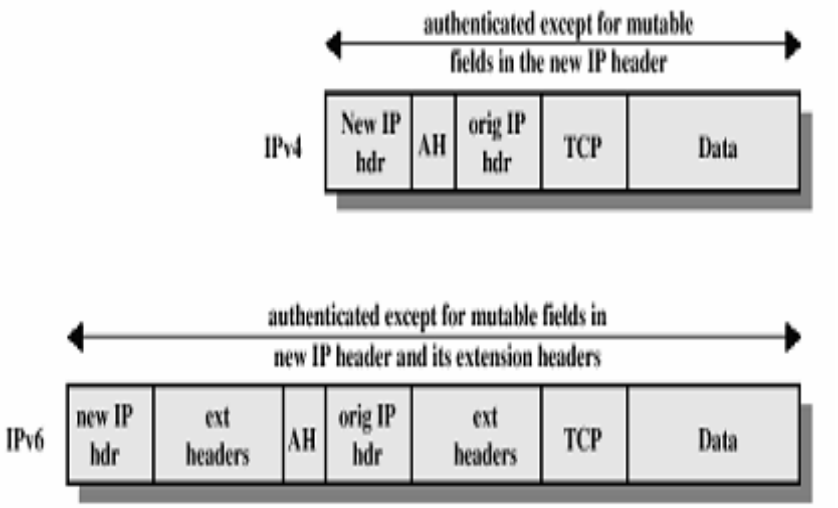


FIG.3.2-29 Modo Túnel de AH

Autor: Investigador
Fuente http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

3.2.2.4 ALGORITMO DE AUTENTIFICACION

AH utiliza algoritmos conocidos como HMAC (códigos de autenticación de mensajes con valores hash) AH lleva un campo (Integrity Check Value) para comprobar la integridad del paquete y que nadie lo puede manipular durante el trayecto. El valor de ese campo está dado por algoritmos de encriptación tales

como MD5 o SHA-1. Permite incorpora una clave secreta mientras se crea el hash.

Para las comunicaciones punto a punto, los algoritmos de autentificación más aptos incluyen claves con Código de Autentificación de Mensaje (MACs) basados en algoritmos de encriptación simétricos (por ejemplo, 3DES) o funciones hash unidireccionales (MD5 o SHA-1).

ALGORITMO HMAC MD5

El algoritmo MD5 es una función matemática de un solo sentido. Aplicado a un bloque de datos, éste produce una representación única de 128 bits de él. El resultado obtenido es una representación comprimida o codificada de un bloque más grande de datos. Cuando se usa de esta manera, MD5 garantiza sólo la integridad en los datos. Un mensaje codificado es sometido a un proceso de cálculo partiendo de un bloque de datos (como pueden ser datagramas IP) antes de que se envíe y otra vez después de que los datos hayan sido recibidos.

Si los dos compendios calculados son iguales, entonces el bloque de datos no tuvo alteración alguna durante la transmisión (suponiendo que hubiese habido una transmisión maligna).

La autenticidad puede ser garantizada mediante el uso de llaves secretas cuando se calcula el mensaje codificado. El método HMAC usa el algoritmo básico MD5 para calcular los mensajes codificados, pero opera en bloques de datos de 64 bytes que sirven, a su vez como entrada de un bloque entero de datos. Este también usa una llave secreta (conocida sólo por los sistemas que se están comunicando) cuando se realiza el cálculo de la codificación

En un sistema de intercambio de datagramas utilizando HMAC-MD5, el emisor previamente intercambiará la llave secreta, para calcular primero una serie de compendios MD5 de 16 bits por cada bloque de 64 bytes del datagrama.

El datagrama se envía al receptor, quien debe también conocer el valor de la llave secreta para calcular el mensaje codificado correcto y compararlo con el mensaje codificado recibido por autentificación. Si los valores coinciden, se concluye que el

datagrama no fue alterado durante su tránsito por la red, y además, éste fue enviado sólo por otro sistema compartiendo el conocimiento de la llave secreta.

Hay que hacer notar que la utilidad de esta técnica se basa en la presunción de que sólo el verdadero emisor (y no un impostor) tiene conocimiento de la llave privada compartida.

El algoritmo MD5 se detalla su funcionalidad en la criptografía en el **punto 3.2.4.3** de este capítulo

3.2.3 CABECERA DE SEGURIDAD ENCAPSULADA (ESP)

El objetivo principal del protocolo ESP (Encapsulating Security Payload) es proporcionar confidencialidad, para ello especifica el modo de cifrar los datos que se desean enviar y cómo este contenido cifrado se incluye en un datagrama IP. Adicionalmente, puede ofrecer los servicios de integridad y autenticación del origen de los datos incorporando un mecanismo similar al de AH.

Dado que ESP proporciona más funciones que AH, el formato de la cabecera es más complejo, este formato consta de una cabecera y una cola que rodean los datos transportados. Dichos datos pueden ser cualquier protocolo IP (por ejemplo, TCP, UDP o ICMP, o incluso un paquete IP completo). El objetivo que se plantea esta cabecera es, precisamente, ocultar la información.

La función de cifrado dentro del protocolo ESP es desempeñada por un algoritmo de cifrado de clave simétrica. Típicamente se usan algoritmos de cifrado bloque, de modo que la longitud de los datos a cifrar tiene que ser un múltiplo del tamaño de bloque (8 o 16 byte, en la mayoría de los casos).

El algoritmo de cifrado en bloques se detalla su funcionalidad en la criptografía en el **punto 3.2.4.1.1** de este capítulo

3.2.3.1 FUNCIONAMIENTO DE ESP

La cabecera de Carga de Seguridad Encapsulada (ESP) está diseñada para proporcionar un conjunto de servicios de seguridad. Que puede ser aplicado solo, o en conjunto con la Cabecera de Autentificación (AH) o en forma anidada, por ejemplo, a través del uso del modo túnel.

La cabecera ESP se inserta antes que la cabecera IP y después que la cabecera de protocolo de capa superior (en modo transporte) o después de una cabecera IP encapsulada (en modo túnel).

ESP es usado para proporcionar confidencialidad, autentificación del origen de los datos, integridad sin conexión, un servicio de anti-replay y confidencialidad limitada del flujo de tráfico.

El conjunto de servicios proporcionados depende de las opciones seleccionadas al momento del establecimiento de la Asociación de Seguridad (SA) y de dónde esté localizada la implementación. La confidencialidad puede ser seleccionada independientemente del resto de los servicios. No obstante el uso de la confidencialidad sin integridad/autentificación (en ESP o AH) puede subordinar tráfico hacia ciertos tipos de ataques activos que podrían ser fáciles de conocer el servicio de confidencialidad.

La autentificación del origen de los datos y la integridad sin conexión son servicios que están unidos y son ofrecidos como una opción junto con la confidencialidad (opcional). La confidencialidad del flujo de tráfico requiere de la selección del modo túnel, y es más efectiva si esta implementada en una puerta de enlace donde la agregación de tráfico puede encubrir patrones verdaderos del originador y del destinatario. Se debe tener en cuenta que la confidencialidad y la autentificación son opcionales, al menos una de ellas debe ser seleccionada.

En la figura 3.2-30 se puede ver como se realiza el funcionamiento de ESP

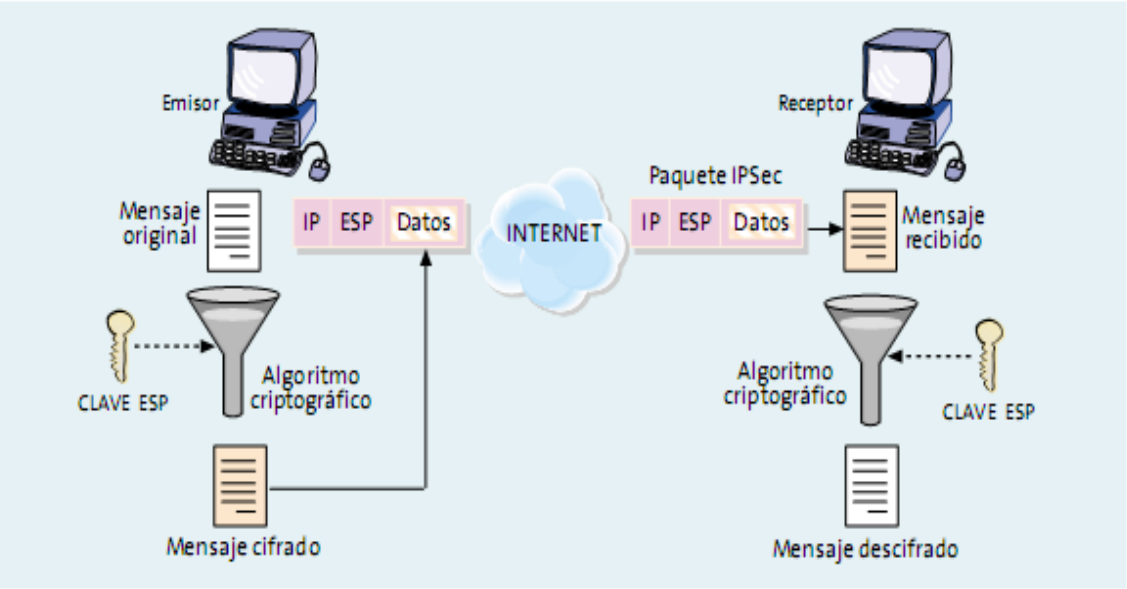


FIG.3.2-30 Funcionamiento de ESP

Autor: Investigador
Fuente http://www.telefonica.es/on/io/es/atencion/tutoriales_articulos/pdf/IPSec.pdf

En la Figura se representa cómo el protocolo ESP permite enviar datos de forma confidencial. El emisor toma el mensaje original, lo cifra, utilizando una clave determinada, y lo incluye en un paquete IP, a continuación de la cabecera ESP. Durante el tránsito hasta su destino, si el paquete es interceptado por un tercero sólo obtendrá un conjunto de bits ininteligible. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales. Está claro que la seguridad de este protocolo reside en la robustez del algoritmo de cifrado, es decir, que un atacante no puede descifrar los datos sin conocer la clave, así la clave ESP únicamente la conocen el emisor y el receptor.

La distribución de claves de forma segura es, por consiguiente un requisito esencial para el funcionamiento de ESP y también de AH, como se ha visto anteriormente. Es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de hash y como en el resto de parámetros comunes que utilizan. Esta labor de puesta en contacto y negociación es realizada por un protocolo de control, denominado IKE, que se verá más adelante en este capítulo.

3.2.3.2 ESTRUCTURA DE ESP

El formato o estructura de ESP está basada en varios campos que contendrán diferentes bits y cada uno de estos campos tienen una función importante en la cabecera de IPv6. En la figura 3.2-31 se puede ver como se determinan cada campo.

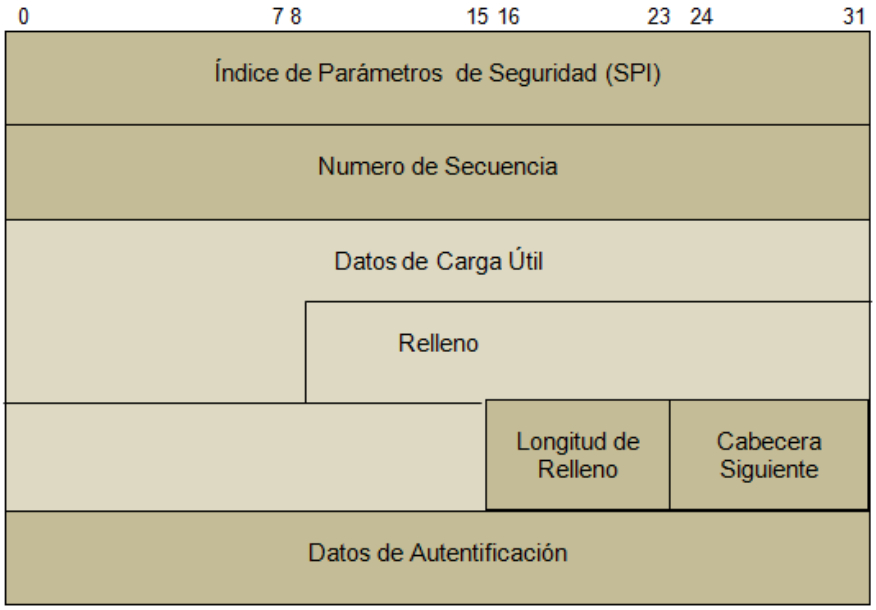


FIG.3.2-31 Estructura de ESP

Autor: Investigador
Fuente: http://es.wikipedia.org/wiki/IPsec

Campo Índice de Parámetros de Seguridad

Identifica los parámetros de seguridad en combinación con la dirección IP. La necesidad del SPI se hace evidente cuando tiene más de una comunicación con la misma dirección IP de destino y protocolo de seguridad (AH o ESP)

Campo Número de Secuencia

Es un número siempre creciente, utilizado para evitar ataques de repetición. Este campo es obligatorio y debe estar siempre presente incluso si el receptor elige no habilitar el servicio de anti- replay para una SA específica. El procesamiento del

campo Número de Secuencia esta a criterio del receptor, es decir, el emisor debe transmitir siempre este campo, pero el receptor no necesita actuar sobre él.

Campo Datos de Carga Útil

Es un campo de longitud variable que contiene los datos (del paquete IP original) descritos por el campo siguiente cabecera, es obligatorio y debe tener una longitud de un número entero de Bytes.

Campo Relleno

El relleno se basa en 0 a 255 octetos Este es el relleno para la encriptación, para ampliar los datos de carga útil con un tamaño que se ajusta a la encriptación de cero a la izquierda tamaño de bloque, y para alinear el siguiente campo.

Campo Longitud de Relleno

Este tipo de campo indica el número de bytes de relleno El rango de valores válidos es de 0 a 255 bytes, donde un valor de cero indica que no hay bytes de relleno presentes. El campo Longitud de Relleno es obligatorio

Campo Siguiente Cabecera

Identifica el protocolo de los datos transferidos.

Campo Datos de Autentificación

Contiene los datos utilizados para autenticar el paquete. En este campo determina la longitud variable y contiene el Valor de Comprobación de Integridad (ICV) calculado sobre el paquete ESP menos, los datos de Autentificación.

3.2.3.3 LOCALIZACION DE ESP

La localización de la cabecera de seguridad encapsulada se puede hacer de dos formas: Modo de Transporte y Modo Túnel.

Modo de Transporte ESP

En este modo el contenido transportado dentro del datagrama AH o ESP son datos de la capa de transporte (por ejemplo, datos TCP o UDP). Por tanto, la cabecera IPSec se inserta inmediatamente a continuación de la cabecera IP y antes de los datos de los niveles superiores que se desean proteger. El modo transporte tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec

En la figura 3.2-32 se mostrará cómo se determina el modo transporte para IPv4 e IPv6.

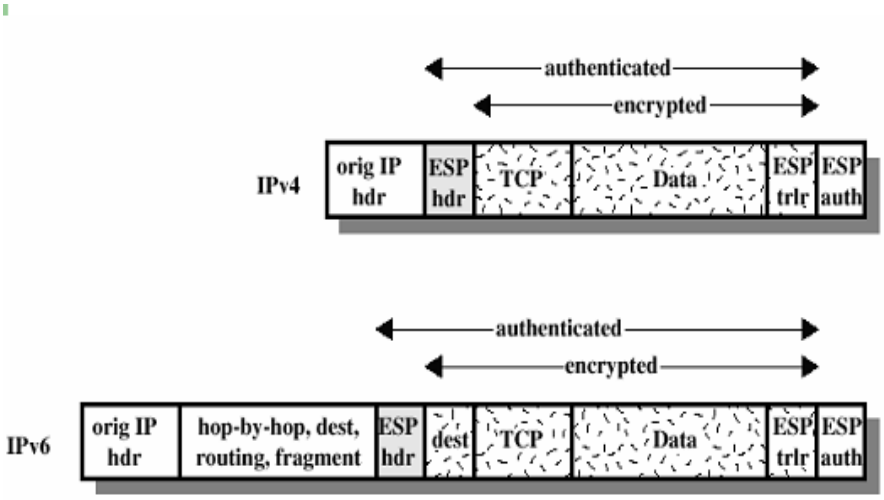


FIG.3.2-32 Modo Transporte de ESP

Autor: Investigador
Fuente http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

Modo Túnel

En éste modo el datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

El modo túnel es empleado principalmente por los gateway IPSec, con objeto de identificar la red que protegen bajo una misma dirección IP y centralizar de este modo el procesado del tráfico IPSec en un equipo.

El modo túnel también es útil, cuando se utiliza junto con ESP, para ocultar la identidad de los nodos que se están comunicando. Otra aplicación del modo túnel,

tanto con ESP como con AH, es poder establecer Redes Privadas Virtuales (RPV) a través de redes públicas, es decir, interconectar de forma segura redes de área local, incluso en el caso de que éstas usen direccionamiento privado o no legal en Internet**.**

En la figura 3.2-33 se mostrará cómo se determina el modo túnel para IPv4 e IPv6.

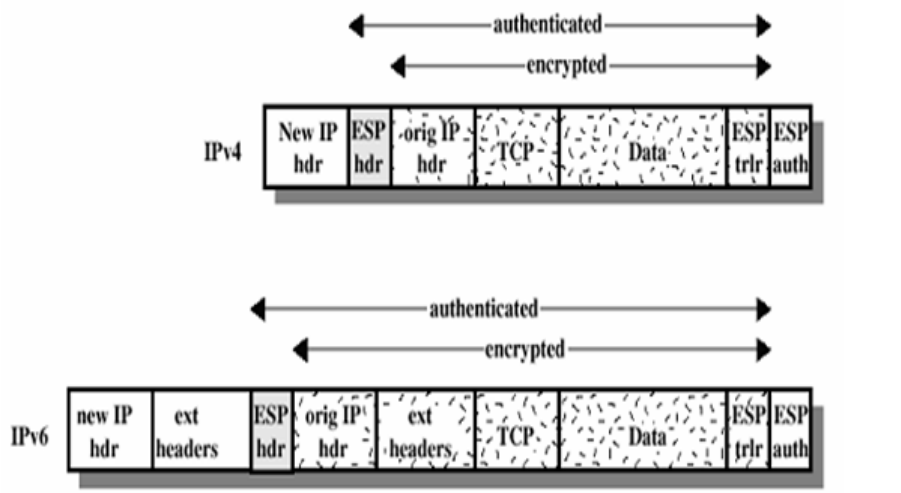


FIG.3.2-33 Modo Túnel de ESP

Autor: Investigador
Fuente http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

3.2.3.4 ALGORITMO DE ENCRIPTACION Y AUTENTIFICACION

Los algoritmos de encriptación que se usa para la implementación obligatoria son los siguientes:

- DES en modo CBC.
- HMAC con MD5.
- HMAC con SHA-1.
- Algoritmo de autenticación NULL.
- Algoritmo de encriptación NULL.

Pero también se pueden usar otros algoritmos.

ALGORITMO DE ENCRIPTACION

El algoritmo de encriptación empleado, es especificado por la SA. ESP está diseñado para usarse con algoritmos de encriptación simétricos. Debido a que los paquetes IP pueden llegar en desorden, cada paquete debe llevar necesariamente algún tipo de dato para permitir que el receptor establezca la sincronización criptográfica para la desencriptación.

Estos datos se pueden llevar explícitamente en el campo carga útil. Puesto que ESP establece normas para el relleno del texto plano, los algoritmos de encriptación empleados con ESP pueden exhibir características de encriptación en modo bloque o de flujo (secuencial). Se debe tener en cuenta que la encriptación (confidencialidad) es opcional, este algoritmo puede ser "NULL".

ALGORITMO DE AUTENTIFICACION

El algoritmo de autentificación empleado esta especificado por la SA. Para la comunicaciones punto a punto, los algoritmos de autentificación más aptos incluyen claves con Código de Autentificación de Mensaje (MACs) basados en algoritmos de encriptación simétricos (por ejemplo, 3DES) o funciones hash unidireccionales (ejemplo, MD5 o SHA-1). Para comunicación multicast, los algoritmos hash unidireccionales combinados con algoritmos de firmas asimétricas son apropiados, aunque las consideraciones de funcionamiento y de espacio actual pueden imposibilitar el uso de tales algoritmos.

Este tipo de algoritmo simétrico o asimétrico se detallará con claridad en el punto **3.2.4.1** y **3.2.4.2** de **Criptografía**.

3.2.4 CRIPTOGRAFIA

En este punto del capítulo se detalla los tipos de criptografías que son utilizados en las distintas cabeceras mencionadas en los puntos anteriores. Por esta razón es necesario mencionar su significado y/o definición para poder entender este tema.

A partir de la evolución de las computadoras, la criptografía fue ampliamente divulgada, empleada y modificada, y se constituyó luego con algoritmos matemáticos. Además de mantener la seguridad del usuario, la criptografía preserva la integridad de la web, la autenticación del usuario así como también la del remitente, el destinatario y de la actualidad del mensaje o del acceso. Las llaves que se puede utilizar en la criptografía pueden ser:

Simétricas: Es la utilización de determinados algoritmos para descifrar y encriptar (ocultar) documentos. Son grupos de algoritmos distintos que se relacionan unos con otros para mantener la conexión confidencial de la información.

Asimétricas: Es una fórmula matemática que utiliza dos llaves, una pública y la otra privada. La llave pública es aquella a la que cualquier persona puede tener acceso, mientras que la llave privada es aquella que sólo la persona que la recibe es capaz de descifrar.

Criptografía es la técnica que protege documentos y datos. Funciona a través de la utilización de cifras o códigos para escribir algo secreto en documentos y datos confidenciales que circulan en redes locales o en internet. Una de las partes esenciales es saber que significa cifrado.

Cifrado

Proceso de camuflar un mensaje o datos de forma que se oculte su contenido. Método para formar un mensaje oculto. El cifrado se utiliza para transformar un mensaje legible, denominado texto plano (también denominado texto no cifrado o texto sin formato) en un mensaje ilegible, codificado u oculto, denominado texto cifrado. Solamente aquel usuario con una clave de decodificación puede convertir dicho texto en el texto original.

Hoy en día la criptografía es fundamental para el desarrollo de las tecnologías de la información y las comunicaciones, puesto que las redes (y particularmente Internet) ha ido evolucionando. Por lo tanto son necesarios métodos criptográficos eficientes y robustos para mantener la privacidad.

3.2.4.1 CRIPTOGRAFIA SIMETRICA O PRIVADA

La criptografía simétrica es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes. Las dos partes que se comunican se deben poner de acuerdo sobre la clave a usar. Una vez ambas tienen acceso a esta clave, el remitente cifra un mensaje usándola, lo envía al destinatario, y éste lo descifra con la misma clave.

Un intercambio de claves proporciona simetría si cualquier parte puede iniciar el intercambio, y los mensajes intercambiados pueden cruzarse en la trayectoria sin afectar la clave generada (ISAKMP). En este tipo de criptografía tanto el emisor como el receptor del mensaje han de conocer la clave y esta clave sirve tanto para encriptar como para desencriptar los mensajes.

Las principales ventajas de esta criptografía son:

- Presentan una longitud de clave considerablemente menor que los algoritmos asimétricos
- Requieren menos recursos computacionales que los algoritmos asimétricos.
- Usa una clave única que sirve tanto para desencriptar como para encriptar.
- El cálculo de la clave no requiere que cada parte sepa quien inició el intercambio (ISAKMP).
- Requiere menos recursos de ancho de banda que los algoritmos asimétricos.

Las principales desventajas de esta criptografía son:

- La simetría en el protocolo de administración de claves puede proporcionar vulnerabilidad a los ataques de reflexión (reflection attacks) (ISAKMP).
- La clave es generada en uno de los extremos de la comunicación, por ende si no se confía en él, este método no serviría.
- Para ser empleados en comunicaciones la clave debe estar tanto en el emisor como en el receptor, lo cual lleva a preguntar cómo transmitir la clave de forma segura si tiene un canal inseguro como Internet.

Este tipo de algoritmos es utilizado por (ESP) para encriptar la información. La Figura 3.2-34 muestra un esquema conceptual de un sistema simétrico.

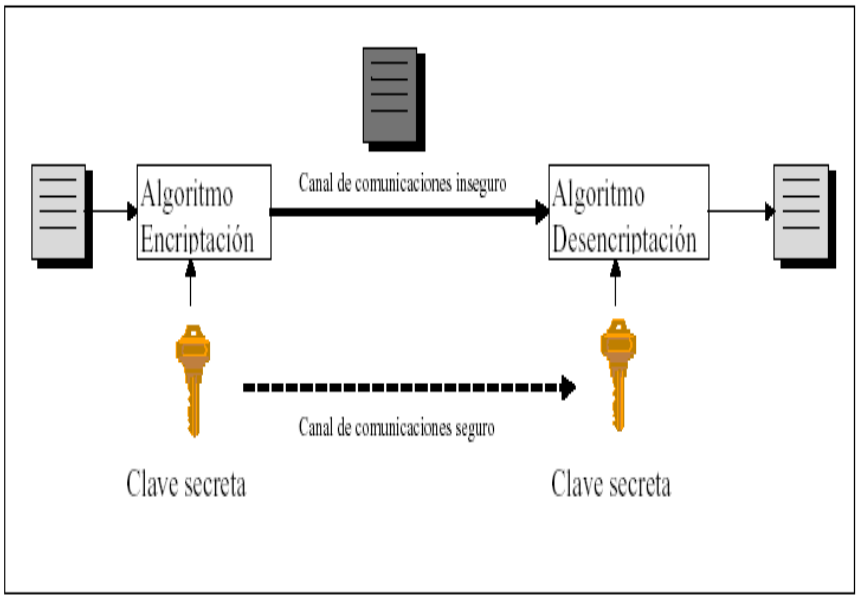


FIG.3.2-34 Criptografía de Sistema Simétrico

Autor: Investigador
Fuente http://www.uv.es/~montanan/redes/trabajos/algoritmos-criptograficos.ppt

Los sistemas de claves simétricos se clasifican en cifrado por Bloque o por Flujo

3.2.4.1.1 CIFRADO EN BLOQUES

Esta técnica consiste básicamente en dividir el mensaje en bloques de tamaño fijo, y aplicar la función de cifrado a cada uno de ellos. Se debe tener en cuenta lo que ocurre cuando la longitud de la cadena que quiere cifrar no es un múltiplo exacto del tamaño de bloque. Entonces tiene que añadir información al final para que sí lo sea.

El mecanismo más sencillo consiste en rellenar con ceros el último bloque que se codifica. El problema ahora consiste en saber cuándo se descifra por dónde hay que cortar. Lo que se suele hacer es añadir como último byte del último bloque el número de bytes que se han añadido.

Esto tiene el inconveniente de que si el tamaño original es múltiplo del bloque, hay que alargarlo con otro bloque entero. Por ejemplo, si el tamaño de bloque fuera 64 bits, y sobran cinco bytes al final, se añadirá dos ceros y un tres, para completar los ocho bytes necesarios en el último bloque. Si por el contrario no sobrara nada, tendrá que añadir siete ceros y un ocho

En la Tabla 3.2-7 Se demuestra cómo se realiza el relleno de los bytes del último bloque, al emplear un algoritmo por bloques

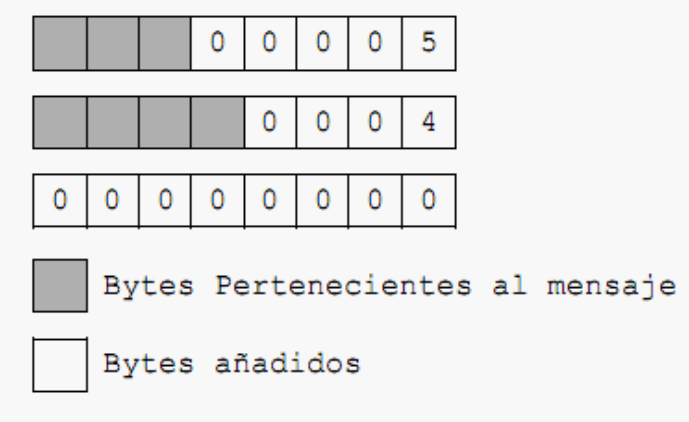


Tabla.3.2-7 Relleno de los bytes en el algoritmo de cifrado por bloques

Autor: Investigador
Fuente http://www.uv.es/~montanan/redes/trabajos/algoritmos-criptograficos.ppt

Los Modos principales de operación para algoritmos de cifrado por bloques son: ECB, CBC, CFB.

Modo ECB

El modo ECB (Bloque de Código Electrónico) simplemente subdivide la cadena que se quiere codificar en bloques de tamaño adecuado y se cifran todos ellos empleando la misma clave.

Permite codificar los bloques independientemente de su orden, lo cual es adecuado para codificar bases de datos o ficheros en los que se requiera un acceso aleatorio. También es resistente a errores, es decir si uno de los bloques sufriera una alteración, el resto quedaría intacto.

También si el mensaje presenta patrones repetitivos, el texto cifrado también los presentará, y eso es peligroso, sobre todo cuando se codifica información muy redundante (como ficheros de texto), o con patrones comunes al inicio y final (como el correo electrónico). Un atacante puede en estos casos efectuar un ataque estadístico y extraer bastante información.

Otro riesgo bastante importante que presenta el modo ECB es el de la sustitución de bloques.

El atacante puede cambiar un bloque sin mayores problemas, y alterar los mensajes incluso desconociendo la clave y el algoritmo empleados. Simplemente se escucha una comunicación de la que se conozca el contenido, como por ejemplo una transacción bancaria a una cuenta corriente. En la siguiente figura 3.2-35 se muestra como es el funcionamiento del modo ECB

FIG.3.2-35 Funcionamiento del modo ECB

Autor: Investigador
Fuente: http://www.uv.es/~montanan/redes/trabajos/algoritmos-criptograficos.ppt

Modo CBC

El modo CBC (Concatenación de Bloques Cifrados) incorpora un mecanismo de retroalimentación en el cifrado por bloques. Esto significa que la codificación de bloques anteriores condiciona la codificación del bloque actual, por lo que será imposible sustituir un bloque individual en el mensaje cifrado.

En cualquier caso, dos mensajes idénticos se codificarán de la misma forma usando el modo CBC. Más aún, dos mensajes que empiecen igual se codificarán igual hasta llegar a la primera diferencia entre ellos.

En la siguiente figura 3.2-36 se muestra el funcionamiento del modo CBC.

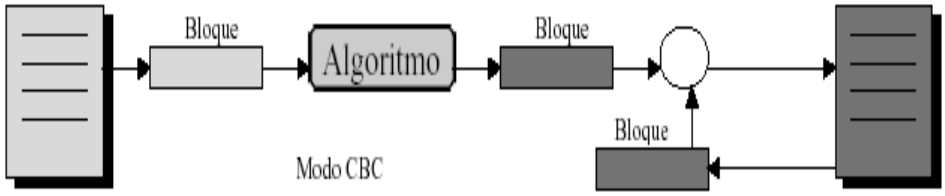


FIG.3.2-36 Funcionamiento del modo CBC

Autor: Investigador
Fuente: http://www.uv.es/~montanan/redes/trabajos/algoritmos-criptograficos.ppt

Modo CFB

El modo de operación CFB (Cipher-Feedback Mode) permitirá codificar la información en unidades inferiores al tamaño del bloque, lo cual permite aprovechar totalmente la capacidad de transmisión del canal de comunicaciones, manteniendo además un nivel de seguridad adecuado.

El modo CFB no empieza a codificar (o decodificar) hasta que no se tiene que transmitir (o se ha recibido) un bloque completo de información. Esta circunstancia puede convertirse en un serio inconveniente, por ejemplo en el caso de terminales, que deberían poder transmitir cada carácter que pulsa el usuario de manera individual.

En la siguiente figura 3.2-37 se muestra el funcionamiento del modo CFB.

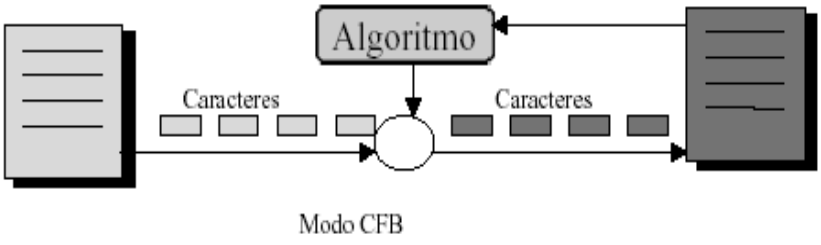


FIG.3.2-37 Funcionamiento del modo CFB

Autor: Investigador
Fuente http://www.uv.es/~montanan/redes/trabajos/algoritmos-criptograficos.ppt

3.2.4.1.1.1 ALGORITMO CRIPTOGRAFICO POR BLOQUES

Los principales algoritmos criptografía por bloques son:

DES (Data Encryption Standard)

Es un algoritmo de cifrado, es decir un método para cifrar información. Este algoritmo simétrico encripta bloques de 64 bits de longitud con una clave de 64 bits de longitud. Dentro de la clave el último bit de cada byte es de paridad, con lo cual tiene la clave en realidad es de **56 bits**, esto hace que haya 2^56 posibles claves para este algoritmo.

Dependiendo de la naturaleza de la aplicación DES puede operar en modo CBC, ECB, CFB.

Dentro de este algoritmo del DES tiene unas pocas claves débiles y semidébiles. Son las claves que causan que el modo de cifrado de DES funcione de manera idéntica al modo de descifrado de DES.

3DES

Para evitar el problema de la llave corta y continuar utilizando DES, existe un sistema basado en tres iteraciones del algoritmo, llamado Triple DES (3DES) o TDES que utiliza una llave de **128 bits** y es compatible con el DES simple . Por ende este algoritmo realiza tres veces el DES, aumentando la longitud de clave a 192 bits (64 x 3).

AES

Advanced Encryption Standard (AES), es un esquema de cifrado por bloques adoptado para diseñar, manejar longitudes de clave y de bloque variables, ambas comprendidas entre los **128 y los 256 bits**. Su interés radica en que todo el proceso de selección, revisión y estudio, se ha efectuado de forma pública y abierta, lo cual convierte a AES en un algoritmo perfectamente digno de la confianza de todos.

Este diseño se radica en tres puntos fundamentales:

- La máxima resistencia a ataques
- Velocidad y compacto para varias plataformas informáticas
- Simplicidad del diseño

IDEA

El algoritmo IDEA (International Data Encryption Algorithm) es el mejor y más seguro algoritmo simétrico disponible en la actualidad. Trabaja con bloques de 64 bits de longitud y emplea una clave de 128 bits reales (no hay bits de paridad como en el DES). Como en el caso de DES, se usa el mismo algoritmo tanto para cifrar como para descifrar. IDEA es un algoritmo bastante seguro, y hasta ahora se ha mostrado resistente a multitud de ataques, entre ellos el criptoanálisis diferencial. No presenta claves débiles, y su longitud de clave hace imposible en la práctica un ataque por fuerza bruta.

3.2.4.1.2 CIFRADO EN FLUJO

Este tipo de cifrado permite cifrar mensajes de longitud arbitraria, sin necesidad de dividirlos en bloques para codificarlos por separado. Pero hay que tomar en cuenta que estos no proporcionan seguridad perfecta, debido a los valores arbitrarios, tiene un máximo de algunas secuencias distintas.

3.2.4.1.2.1 ALGORITMO CRIPTOGRAFICO POR FLUJO

Los principales algoritmos criptografía por flujo son:

RC4

Se caracteriza por utilizar la misma información de entrada que cifrará para la generación de un número pseudoaleatorio que utilizará como clave, realizando un XOR entre la entrada y la clave. Esto significa que tanto el cifrado como el

descifrado son operaciones idénticas. No se debe utilizar la misma clave más de una vez

RC4 fue excluido enseguida de los estándares de alta seguridad por los criptógrafos y algunos modos de usar el algoritmo de criptografía RC4 lo han llevado a ser un sistema de criptografía muy inseguro, incluyendo su uso WEP. No está recomendado su uso en los nuevos sistemas, sin embargo, algunos sistemas basados en RC4 son lo suficientemente seguros para un uso común.

MAC

Es una extensión del RC4 que busca asegurar la integridad en los datos mediante el uso de una función MAC es una función que asegura la integridad de los datos, a partir del mensaje genera una secuencia de bits de tal forma que si es modificado, el receptor puede saberlo.

3.2.4.2 CRIPTOGRAFIA ASIMETRICA O PUBLICA

La criptografía asimétrica es el método criptográfico, que usa un par de claves para el envío de mensajes. Las dos claves pertenecen a la misma persona a la que se ha enviado el mensaje.

Una clave es pública y se puede entregar a cualquier persona, la otra clave es privada y el propietario debe guardarla de modo que nadie tenga acceso a ella. Además, los métodos criptográficos garantizan que esa pareja de claves sólo se puede generar una vez, de modo que se puede asumir que no es posible que dos personas hayan obtenido casualmente la misma pareja de claves.

Si el remitente usa la clave pública del destinatario para cifrar el mensaje, una vez cifrado, sólo la clave privada del destinatario podrá descifrar este mensaje, ya que es el único que la conoce. Por tanto se logra la confidencialidad del envío del mensaje, nadie salvo el destinatario puede descifrarlo.

Los sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos.

Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear. Todo lo que se requiere es que, antes de iniciar la comunicación secreta, el remitente consiga una copia de la clave pública del destinatario. Es más, esa misma clave pública puede ser usada por cualquiera que desee comunicarse con su propietario. Por tanto, se necesitarán sólo n pares de claves por cada n personas que deseen comunicarse entre sí.

3.2.4.2.1 ALGORITMOS ASIMETRICOS

Los algoritmos asimétricos poseen dos claves diferentes en lugar de una, la clave privada K_{Pr} y la clave pública K_{Pu}, eliminando el mayor problema de los sistemas de clave privada, dar a conocer únicamente al receptor autorizado la clave usada en el sistema de cifrado/descifrado.

Una de ellas se emplea para codificar, mientras que la otra se usa para decodificar. Dependiendo de la aplicación del algoritmo la clave pública la de cifrado o viceversa. Como se ve se introduce un nuevo problema, la autenticación del origen de los datos. Puesto que todo el mundo conoce la clave pública, se puede enviar un mensaje falseando la procedencia.

En los sistemas de clave privada esto no pasa, ya que la clave la conoce únicamente el emisor y el receptor de la información, asegurando la confidencialidad y la procedencia de la información.

Los principales algoritmos que se usan en este tipo de criptografía son:

Algoritmo de Diffie Hellman

El protocolo Diffie-Hellman permite el intercambio secreto de claves entre dos partes que no han tenido contacto previo, utilizando un canal inseguro, y de manera anónima (no autenticada). Se emplea generalmente como medio para acordar claves simétricas que serán empleadas para el cifrado de una sesión.

Siendo no autenticado, sin embargo provee las bases para varios protocolos autenticados. Su seguridad radica en la extrema dificultad de calcular logaritmos discretos en un campo finito.

La ventaja de este sistema es que no son necesarias llaves públicas en el sentido estricto, sino información compartida por los dos comunicantes. Este algoritmo no proporciona ni autenticación ni cifrado, por ende no suele utilizarse para la protección de datos. Debido a que es uno de los algoritmos más utilizados con IPsec.

- **Los grupos Diffie Hellman**

  Los grupos Diffie Hellman se utilizan para determinar la longitud de los números primos base (del material clave) utilizados durante el proceso de intercambio de claves de Diffie Hellman. La eficacia criptográfica de cualquier clave derivada de este grupo depende en parte de la eficacia del grupo de Diffie Hellman en el que se basan los números primos.

  - El grupo 1 proporciona 768 bits de protección de clave
  - El grupo 2 proporciona 1024 bits
  - El grupo 2048 proporciona 2048 bits.

  Cuando se utiliza un grupo más seguro, la clave derivada del intercambio Diffie Hellman es más segura y es más difícil que un intruso la averigüe. Si se especifican grupos no coincidentes en cada interlocutor, no será posible la negociación. El grupo no se puede cambiar durante la negociación.

Algoritmo RSA

En criptografía, RSA es un sistema criptográfico de clave pública. En la actualidad RSA es el primer y más utilizado algoritmo de este tipo y es válido tanto para cifrar como para firmar digitalmente.

La seguridad de este algoritmo radica en el problema de la factorización de números enteros. Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto.

Como en todo sistema de clave pública, cada usuario posee dos claves de cifrado: una pública y otra privada. Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

Se cree que RSA será seguro mientras no se conozcan formas rápidas de descomponer un número grande en producto de primos. La computación cuántica podría proveer de una solución a este problema de factorización

3.2.4.3 FUNCIONES DEL HASH

Este tipo de algoritmo permite generar un valor de resumen (hash) de algún dato, como una clave de mensaje o de sesión. Con un buen algoritmo de hash, los cambios que se produzcan en los datos de entrada pueden cambiar todos los bits del valor hash resultante, por lo que estos valores son útiles para detectar cualquier modificación en un objeto de datos, como un mensaje.

Además, un buen algoritmo de hash hace que sea computacionalmente imposible crear dos entradas que tengan el mismo valor hash. Los algoritmos de hash comunes son MD2, MD4, MD5 y SHA-1. Estos algoritmos también se llaman funciones hash o MDC (Código Detector de Modificaciones).

Los más utilizados son MD5 y SH1.

Algoritmo MD5

En criptografía, MD5 (Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

Resultado de una serie de mejoras sobre el algoritmo MD4 (el cual es una función hash que produce una secuencia de 128 bits asociados al mensaje original), diseñado por Ron Rivest, procesa los mensajes de entrada en bloques de 512 bits, y produce una salida de 128 bits.

MD5 se utilizan extensamente en el mundo del software para proporcionar la seguridad de que un archivo descargado de Internet no se ha alterado. Esto protege al usuario contra los Caballos de Troya y virus que algún otro usuario malicioso pudiera incluir en el software. La comprobación de un archivo descargado contra su suma MD5 no detecta solamente los archivos alterados de una manera maliciosa, también reconoce una descarga corrupta o incompleta

Algoritmo SHA-1

El algoritmo SHA-1 fue desarrollado por la NSA (Agencia Nacional de Seguridad de USA), para ser incluido en el estándar DSS (Digital Signature Standard). Produce firmas de 160 bits, a partir de bloques de 512 bits del mensaje original. A diferencia de MD5, SHA-1 emplea cinco registros de 32 bits en lugar de cuatro.

3.3 PROTOCOLO DE INTERCAMBIO DE CLAVES EN INTERNET (IKE)

El protocolo de Intercambio de Claves en Internet (IKE) resuelve el problema más importante del establecimiento de comunicaciones seguras como la autenticación de los participantes y el intercambio de claves simétricas.

El protocolo IKE se implementa a través de servidores de espacio de usuario, y no se implementan en el sistema operativo. El protocolo IKE emplea el puerto 500 UDP para su comunicación.

Este tipo de protocolo funciona en dos fases. La primera fase establece un ISAKMP SA (Asociación de seguridad del protocolo de gestión de claves de asociaciones de seguridad en Internet). En la segunda fase, el ISAKMP SA se emplea para negociar y establecer las SAs de IPsec.

- La primera fase suele soportar dos modos distintos: modo principal y modo agresivo. Ambos modos autentifican al participante en la comunicación y establecen un ISAKMP SA, pero el modo agresivo sólo usa la mitad de mensajes para alcanzar su objetivo.

Esto sin embargo, tiene sus desventajas, ya que el modo agresivo no soporta la protección de identidades y, por lo tanto es susceptible a un ataque.

- En la segunda fase, el protocolo IKE intercambia propuestas de asociaciones de seguridad y negocia asociaciones de seguridad basándose en la ISAKMP SA.

  La ISAKMP SA proporciona autenticación para protegerse de ataques. Esta segunda fase emplea el modo rápido. Normalmente, dos participantes de la comunicación sólo negocian una ISAKMP SA, que se emplea para negociar varias IPsec SAs unidireccionales.

3.3.1 FUNCIONAMIENTO DEL PROTOCOLO IKE

Para el funcionamiento de este protocolo se debe tener en cuenta los conceptos anteriores que se ha detallado para poder entender el funcionamiento de IKE.

Un concepto esencial en IPSec es el de asociación de seguridad (SA) es un canal de comunicación unidireccional que conecta dos nodos, a través del cual fluyen los datagramas protegidos mediante mecanismos criptográficos acordados previamente. Al identificar únicamente un canal unidireccional, una conexión IPSec se compone de dos SAs, una por cada sentido de la comunicación.

Se conoce que ambos extremos de una asociación de seguridad deben tener conocimiento de las claves, así como del resto de la información que necesitan para enviar y recibir datagramas AH o ESP. Tal como se ha indicado anteriormente, es necesario que ambos nodos estén de acuerdo tanto en los algoritmos criptográficos a emplear como en los parámetros de control. Esta operación puede realizarse mediante una configuración manual, o mediante algún protocolo de control que se encargue de la negociación automática de los parámetros necesarios; a esta operación se le llama negociación de SAs.

Una característica importante de IKE es su utilidad que no se limita a IPSec, sino que es un protocolo estándar de gestión de claves que podría ser útil en otros protocolos.

IKE es un protocolo híbrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley y utiliza un algoritmo Diffie Hellman para intercambio de claves y permite crear una sesión compartida secreta de las claves. ISAKMP define de forma genérica el protocolo de comunicación y la sintaxis de los mensajes que se utilizan en IKE, mientras que Oakley especifica la lógica de cómo se realiza de forma segura el intercambio de una clave entre dos partes que no se conocen previamente. En el siguiente grafico 3.3-38 se determina el funcionamiento de IKE

Los protocolos ISAKMP se detallarán en el punto 3.4

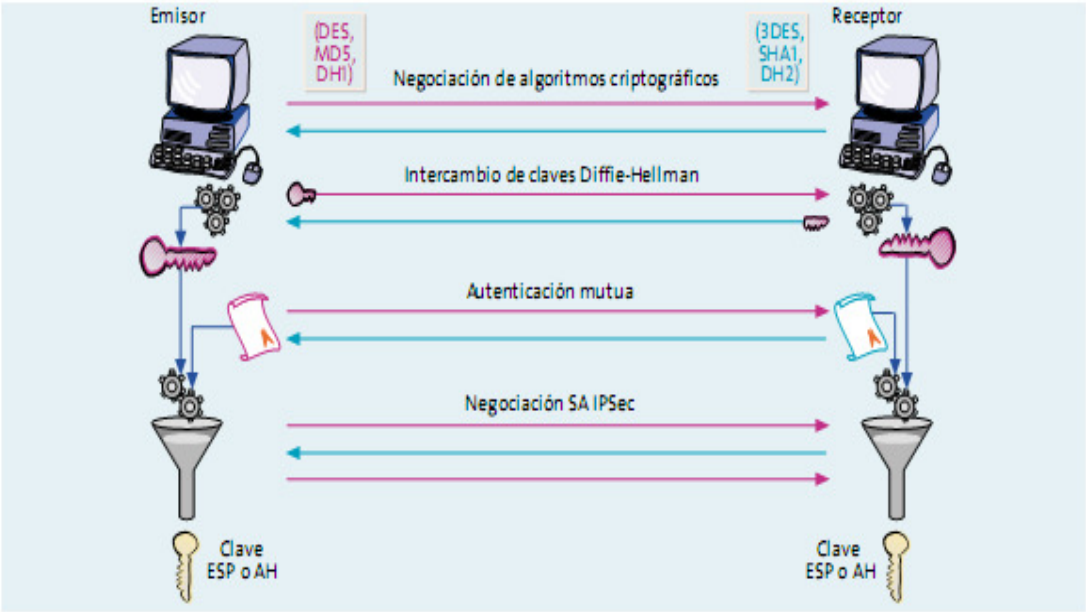


FIG.3.3-38 Funcionamiento del Protocolo IKE

Autor: Investigador
Fuente: http://www.tesis.ufm.edu.gt/pdf/3930.pdf

3.3.2 ARQUITECTURA DEL PROTOCOLO IKE

El protocolo IKE define en su arquitectura dos fases que determinan la estructura para el establecimiento de un canal auténtico y seguro entre dos usuarios.

Este protocolo utiliza la infraestructura de mensajes del protocolo ISAKMP para el intercambio de mensajes. Para cada una de las fases se debe tener en cuenta la notación con su significado.

HDR:	Cabecera ISAKMP.
HDR*:	Cabecera cifrada
HASH:	Función Hash.
KE:	Valor público Diffie-Hellman.
SA:	Asociación de seguridad.
Ni y Nr:	Valor temporal (Nonce payload).
[Cert] y SIG:	Certificado y firma digital.
ID:	Identificador.
PubK:	Clave pública.
[ ]:	Opcional.

Tabla.3.3-8 Notación con sus significados para la Arquitectura del Protocolo IKE

Autor: Investigador

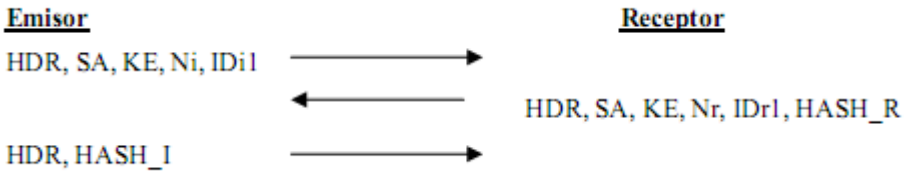
NOTA: La tabla fue creada por el investigador de acuerdo a la documentación.

Fase1:

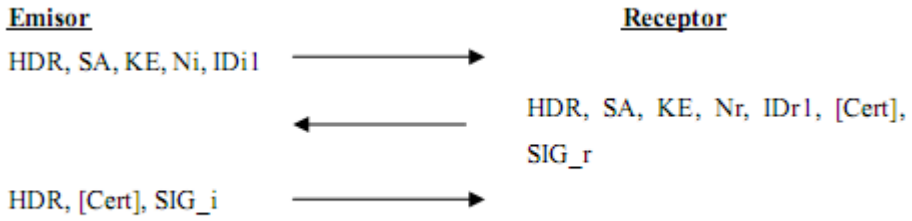
Se negocian las asociaciones de seguridad (SA). Se utiliza el protocolo Diffie-Hellman para el intercambio de una clave común y se establece el algoritmo de cifrado (3DES-CBC), el algoritmo de Hash (MD5) y del sistema de autenticación.

En esta fase tanto el emisor como el receptor quedan autenticados mediante uno de los siguientes cuatro métodos tanto el método principal o agresivo:

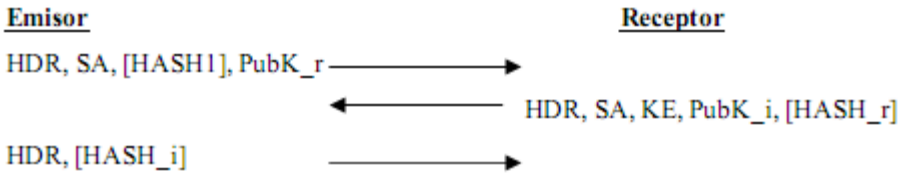
1. Autenticación con claves pre-compartidas (Pre-shared Keys).



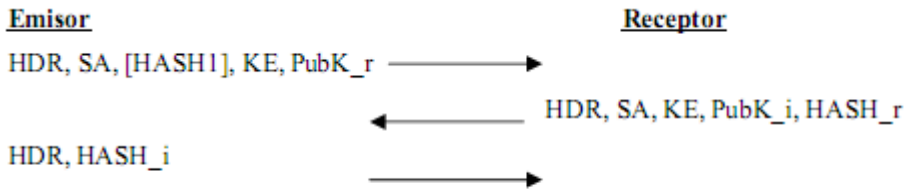
2. Autenticación mediante firmas digitales (Digital Signatures).



3. Autenticación mediante clave pública 1.



4. Autenticación mediante clave pública 2.



Fase 2:

Una vez establecidos los distintos parámetros iníciales (SA) y aprovechando la seguridad de la fase 1, se inicia un modo rápido (Quick Mode) dónde se vuelven a negociar asociaciones de seguridad (SA) con el objetivo de evitar ataques de reutilización (Replay) de los datagramas de la fase 1 por un atacante.

Esta combinación de algoritmos permite mantener una comunicación auténtica y privada entre dos usuarios, el problema principal radica en su complejidad, ya que pese a ser muy flexible es difícil su implementación práctica.

3.3.3 INTERCAMBIO DE CLAVES

Hay dos métodos básicos usados para establecer un intercambio de claves autentificado: El Modo Principal y el Modo Agresivo. Cada uno genera material clave autentificado a partir de un intercambio de Diffie Hellman. El modo principal DEBE ser implementado para establecer un intercambio de claves, en cambio El modo agresivo DEBERIA ser implementado y El modo rápido SE DEBE implementar como mecanismo para generar nuevo material clave y para negociar servicios de seguridad

Modo Principal

El modo principal se utiliza para la confidencialidad y autentificación mediante el uso de algoritmos y autenticación acordados en los Hosts donde se va a realizar la comunicación lo que permite establecer un canal seguro denominado SA.

Es un cambio en la primera fase de IKE / ISAKMP, los dos primeros mensajes que se encuentra en el gráfico 3.3-39 se utilizan para la negociación de la política de seguridad para el intercambio.

Los siguientes dos mensajes se utilizan como material de claves mediante intercambio Diffie Hellman. Los últimos dos mensajes se utilizan para la autenticación de los pares con las firmas o hashes y certificados opcionales.

Los dos últimos mensajes de autenticación están cifrados con la clave previamente negociada y las identidades de las partes están protegidas de miradas indiscretas de usuarios que deseen conocer la clave o el contenido de la información.

En la figura 3.3-39 se determina el funcionamiento del modo principal del protocolo IKE El significado de HDR, IKE entre otras del gráfico están en el punto 3.3.2 Arquitectura del protocolo IKE.

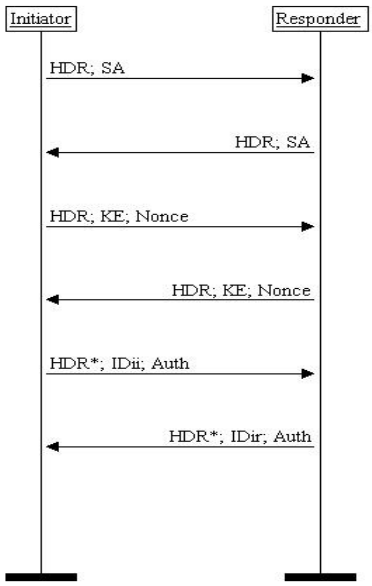


FIG.3.3-39 Modo Principal del Protocolo IKE

Autor: Investigador
Fuente: http://www.niksula.cs.hut.fi/~sjsavola/SoN/essay.html

Modo Agresivo

Modo agresivo tiene la misma funcionalidad del modo principal, pero utiliza la mitad de los mensajes para alcanzar su objetivo y no soporta la protección de identidades por lo que es susceptible a un atacante y transmite la información del usuario de forma clara, permitiendo conocer a los usuarios antes de la autenticación que se va a llevar a cabo. El primer mensaje que se encuentra en el gráfico 3.3-40 negocia la política, intercambian los valores y los datos necesarios para el intercambio de datos para su identificación.

El segundo mensaje autentifica al emisor y llega a la conclusión de la política y el intercambio de datos que se está realizando entre el emisor y el receptor El último mensaje se utiliza para la autenticación del emisor y proporciona una prueba de la participación en el intercambio. En la figura 3.3-40 se determina el funcionamiento del modo agresivo del protocolo IKE

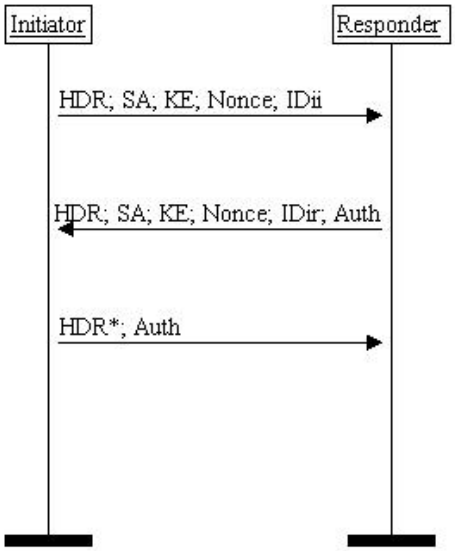


FIG.3.3-40 Modo Agresivo del Protocolo IKE

Autor: Investigador
Fuente: http://www.niksula.cs.hut.fi/~sjsavola/SoN/essay.html

La negociación de SA está limitada en el Modo Agresivo, debido a los requerimientos en la construcción de mensajes, el grupo en el cual el intercambio de Diffie Hellman se ejecuta no puede ser negociado. Además, métodos de autentificación diferentes pueden limitar aun más la negociación de los atributos.

Modo Rápido

El modo rápido se utiliza para el intercambio en la segunda fase de IKE. El modo rápido se utiliza para la negociación de SA y la generación de material de claves nuevas. Todas las cargas útiles, excepto encabezado ISAKMP están cifradas. El intercambio de claves Diffie Hellman se puede hacer para lograr la confidencialidad directa perfecta.

En Modo Rápido, una carga hash debe seguir inmediatamente a la cabecera ISAKMP y una carga SA debe seguir inmediatamente al Hash. Este hash autentifica el mensaje y también proporciona prueba de la actividad.

En la figura 3.3-41 se determina el funcionamiento del modo rápido del protocolo IKE

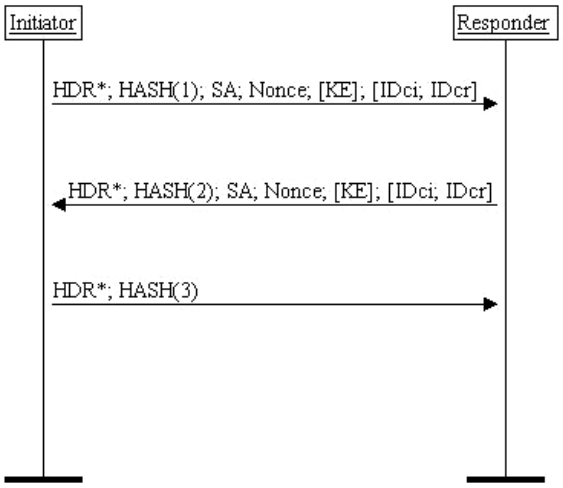


FIG.3.3-41 Modo Rápido del Protocolo IKE

Autor: Investigador
Fuente: http://www.niksula.cs.hut.fi/~sjsavola/SoN/essay.html

3.4 PROTOCOLO DE GESTION DE CLAVES Y ASOCIACION DE SEGURIDADES EN INTERNET (ISAKMP)

Este tipo de protocolo es el escogido para el intercambio de claves y parámetros de seguridad en IPSec, normalmente utiliza IKE para el intercambio de claves, aunque otros métodos pueden ser implementados.

ISAKMP define los procedimientos y formatos de paquetes para establecer, negociar, modificar y eliminar las SA (asociaciones de seguridad). Una Asociación de Seguridad contiene toda la información necesaria para la ejecución de diversos servicios de seguridad de red, como a nivel IP (IPsec AH o ESP), transporte o servicios de la capa de aplicación. ISAKMP define el formato para el intercambio de generación de claves y datos de autenticación. Proporciona un marco coherente para la transferencia de claves y datos de autenticación, que es independiente de la técnica de generación de claves, el algoritmo de cifrado y el mecanismo de autenticación.

3.4.1 FUNCIONAMIENTO DEL PROTOCOLO ISAKMP

El Protocolo de Gestión de Claves y Asociaciones de Seguridad en Internet (ISAKMP), utiliza conceptos de seguridad necesarios para el establecimiento de Asociaciones de Seguridad (SA) y claves criptográficas en un entorno de Internet. Es un protocolo que negocia, establece, modifica y cancela SAs y sus atributos es requerido para la Internet en desarrollo, donde existirán numerosos mecanismos de seguridad y varias opciones para cada mecanismo.

El protocolo de seguridad de manejo de claves debe ser robusto para manejar la generación de claves públicas para la comunidad de Internet y los requerimientos de claves privadas para este tipo de redes que lo requieran.

El Protocolo ISAKMP define los procedimientos para autentificar comunicaciones entre usuarios, la creación y administración de Asociaciones de Seguridad, las técnicas de generación de claves y atenuación de amenazas (como por ejemplo, denegación de servicio y ataques de reenvío). Todo esto es necesario para entablar y mantener comunicaciones seguras en un entorno de Internet.

Negociado el Protocolo ISAKMP

Las Asociaciones de Seguridad deben soportar diversos algoritmos de encriptación, autentificación y mecanismos de establecimiento de claves para IPsec, como así también para otros protocolos de seguridad. Las Asociaciones de seguridad también deben soportar certificados orientados a host para los protocolos de capas inferiores orientados a usuarios para protocolos de capas superiores. Algoritmos y mecanismos independientes se requieren en aplicaciones tales como, e-mail, conexión remota, transferencia de archivos, como sesiones orientadas a protocolos, protocolos de ruteo, y protocolos de capas de enlace.

ISAKMP proporciona una SA común y protocolos de establecimiento de claves para esta gran variedad de protocolos de seguridad, aplicaciones, requerimientos de seguridad y ambientes de redes.

ISAKMP no está sujeto a ningún algoritmo criptográfico especifico, técnica de generación de claves o mecanismos de seguridad. Esta flexibilidad es beneficiosa por numerosas razones.

Primero porque soporta ambientes de comunicaciones dinámicos. Segundo permite la independencia de los mecanismos de seguridad específicos y suministra a los algoritmos un mejor camino migratorio progresivo para mecanismos y algoritmos.

Cuando mejores mecanismos de seguridad son desarrollados o nuevos ataques a algoritmos de encriptación actuales, como los mecanismos de autentificación o intercambios de generación de claves son descubiertos ISAKMP permitirá la actualización de algoritmos y mecanismos sin tener que desarrollar un nuevo protocolo o mejorar el actual.

Fases de la Negociación

ISAKMP ofrece dos fases para la negociación.

La Fase 1:

Dos entidades concuerdan en cómo proteger futuras negociaciones del tráfico entre ellas mismas, estableciendo una SA ISAKMP. Esta SA ISAKMP es luego usada para proteger las negociaciones requeridas por las SA de los Protocolos. Dos entidades pueden negociar (si están activos) múltiples SA ISAKMP.

La Fase 2

De la negociación es usada para establecer la SA para otros protocolos de seguridad. Esta segunda fase puede ser usada para establecer múltiples SA. Las SA establecidas por ISAKMP durante esta fase pueden ser usadas por un protocolo de seguridad para proteger los intercambios de datos o mensajes.

3.4.2 ARQUITECTURA DEL PROTOCOLO ISAKMP

La arquitectura del protocolo ISAKMP se determina en una cabecera donde cada campo realiza una función específica para la seguridad del mensaje. El mensaje de ISAKMP tiene un formato de cabecera fijo, seguido por un número de cargas variables. En la figura 3.4-42 se muestra el formato de la cabecera fija de ISAKMP

FIG.3.4-42 Formato de la Cabecera ISAKMP

Autor: Investigador
Fuente: http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

Los campos de la Cabecera ISAKMP realizan una función específica que son:

Campo Cookie del Emisor

Este campo inicia el establecimiento, modifica, o cancela la SA.

Campo Cookie del Receptor

Este campo responde al requerimiento del establecimiento de una SA, o cancelación de la SA.

Campo Carga siguiente

Indica el tipo de carga en el primer mensaje el formato de cada carga.

Campo Versión Mayores

Indica la versión mayor del protocolo ISAKMP en uso.

Campo Versión Menores

Indica la versión menor del protocolo ISAKMP en uso. Las implementaciones basadas en Internet de ISAKMP debe fijar la versión menor en cero. Las implementaciones nunca deben aceptar paquetes con un número de versión superior a estos, dado que los números de la versión mayor son idénticos.

Campo Tipo de intercambio

Indica el tipo de intercambio usado. Este indica a las computadoras los mensajes y la carga en los intercambios de ISAKMP.

Campo Banderas (Flags)

Indica las opciones específicas que se fijan para los intercambios ISAKMP.

Campo Identificador (ID) de Mensaje

El Identificador de Mensaje solamente se usa para identificar el protocolo durante las negociaciones de la Fase 2. Este valor es generado aleatoriamente por el iniciador de la Fase.

En el caso de establecimientos simultáneos de SA (es decir colisiones), el valor de este campo será probablemente diferente porque son generados independientemente y así dos SAs seguirán con el establecimiento. Sin embargo es improbable de que existan establecimientos simultáneos. Durante las negociaciones de la Fase 1, el valor debe ser cero.

Campo Longitud

Indica la longitud total del mensaje (cabecera más cargas) en octetos. La encriptación puede expandir el tamaño de un mensaje ISAKMP.

3.4.2.1 CABECERA DE CARGA GENERICA DEL PROTOCOLO ISAKMP

La cabecera de carga genérica permite proporcionar una capacidad de encadenamiento de cargas y claramente define los límites de una carga. En la figura 3.4-43 se muestra el formato correspondiente:

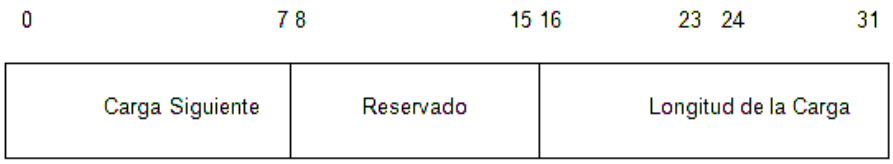


FIG.3.4-43 Formato de la Cabecera de Carga Genérica

Autor: Investigador
Fuente: http://fcqi.tij.uabc.mx/docentes/lpalafox/cursos/segredes/ipsec.pdf

Los campos de la cabecera de la carga genérica son definidos de la siguiente forma:

Campo Carga Siguiente

Permite identificar el tipo de carga de la siguiente carga en el mensaje. Si la carga actual es la última en el mensaje, este campo contendrá el valor cero. Este campo proporciona la capacidad de encadenamiento.

Campo Reservado

No es utilizado, debe contener ceros.

Campo Longitud de la carga

Indica la longitud de la carga actual en octetos, incluyendo la cabecera de carga genérica.

CARGAS DEL PROTOCOLO ISAKMP

Dentro del protocolo ISAKMP se determinan diferentes cargas es necesario conocer el funcionamiento de cada una de ella. Entre estas cargas se determinan las siguientes:

Carga SA

La carga SA es usada para negociar los atributos de seguridad, para indicar el Dominio de Interpretación (DOI) y la situación (el conjunto de información que será utilizado para determinar los servicios de seguridad requeridos) bajo la cual se está llevando a cabo.

Carga de la Propuesta

La Carga de la Propuesta contiene información usada durante la negociación de la SA. La propuesta consiste en mecanismos de seguridad, o trasformaciones, que serán usados para asegurar el canal de comunicaciones.

Carga de Transformación

La Carga de Transformación contiene información usada durante la negociación de la SA. La Carga de Transformación consiste en un mecanismo de seguridad específico, o trasformaciones, con el objetivo de asegurar el canal de comunicación. La carga de Transformación también contiene los atributos SA asociados con la transformación específica.

Carga de Intercambio de Clave

La Carga de Intercambio de Claves soporta una variedad de técnicas de intercambio de claves. Ejemplos de intercambio de claves como Diffie Hellman.

Carga de Identificación

La Carga de Identificación contiene datos específicos del DOI usados para intercambiar información de identificación. Está información es usada para determinar las identidades de los usuarios de la comunicación y puede ser usada para determinar la autentificación de la información.

Carga Hash

La Carga Hash contiene los datos generados por la función hash (seleccionada durante el intercambio del establecimiento de la SA), sobre una cierta parte del mensaje del estado de ISAKMP. Esta carga puede ser usada para verificar la

integridad de los datos en un mensaje ISAKMP, o para la autentificación de las entidades de la negociación.

Carga Nonce

La Carga Nonce contiene información aleatoria para garantizar la vida de la conexión durante un intercambio y para proteger contra ataques de reenvío.

Si el nonce es usado para un intercambio de clave particular, el uso de la carga nonce será dictaminado por el intercambio de claves. El nonce puede ser trasmitido como parte de los datos del intercambio de claves, o como una carga separada.

3.4.3 INTERCAMBIO DE CLAVES DE ISAKMP

Un intercambio es una especificación de un número de mensajes en ISAKMP y los tipos de carga que están contenidos en cada uno de estos mensajes como los servicios de seguridad Hay actualmente 5 tipos de intercambio por defecto definidos por ISAKMP. Los intercambios definen los contenidos y el ordenamiento de los mensajes ISAKMP entre usuarios.

HDR: Es una cabecera de ISAKMP cuyo tipo de intercambio define el ordenamiento de la carga.

SA: Es una carga de negociación de SA con una o más Propuestas y cargas de Transformación.

KE: Es la carga de intercambio de claves.

IDx: Es la carga de Identificación para "x". puede ser "ji" o "ir" para el iniciador y respondedor de ,ISAKMP,

SIG: Es la carga de la firma. Los datos a firmar son específicos del intercambio.

AUTH: Es un mecanismo de autentificación genérico, como HASH o SIG.

NONCE: Es la carga NONCE.

*: Significa encriptación de la carga después de la cabecera ISAKMP.

→ Comunicación desde el "iniciador al respondedor".

← Comunicación desde el "respondedor al iniciador".

Tabla.3.4-9 Notación con sus significados para el Intercambio de Claves de ISAKMP

Autor: Investigador
NOTA: La tabla fue creada por el investigador de acuerdo a la documentación

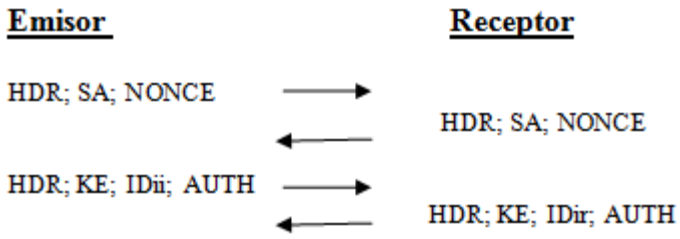
Los diferentes tipos de Intercambios que existen en ISAKMP con su respectivo funcionamiento son:

Intercambio Base

El Intercambio Base está diseñado para permitir que el Intercambio de Claves y la Autentificación puedan relacionarse con la información que se trasmiten simultáneamente.

La combinación del Intercambio de Claves y la información de Autentificación relacionada dentro de un mensaje reduce el número de viajes de ida y vuelta a expensas de no proporcionar protección de identidad. La protección de identidad no es proporcionada porque las identidades se intercambian antes de que un secreto común compartido haya sido establecido, por consiguiente, la encriptación de las identidades no es posible.

El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio Base.



En el primer mensaje (1), el emisor genera una propuesta que considera adecuada para proteger el tráfico en una situación dada. Las cargas, SA, la de la Propuesta, y la de Transformación, son incluidas en la carga SA (para simplificar la notación).

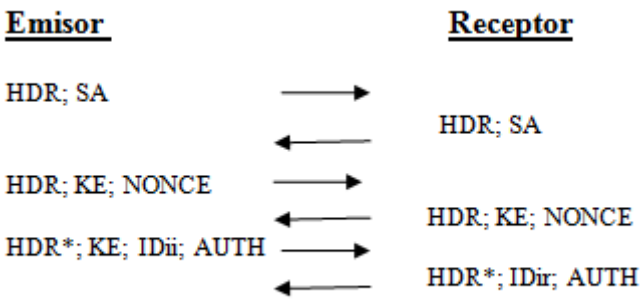
En el segundo mensaje (2), el receptor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación.

En el tercer (3) y cuarto (4) mensaje, el emisor y el receptor, respectivamente intercambian material clave usado para llegar a un secreto común compartido y a la identificación de la información. Esta información es trasmitida bajo la protección de una función de autentificación acordada.

Intercambio de Protección de Identidad

El Intercambio de Protección de Identidad está diseñado para separar la información de Intercambio de Claves de la Identificación y de la información relacionada con la Autentificación.

El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio de Protección de Identidad.



En el primer mensaje (1), el emisor genera una propuesta que considera adecuada para proteger el tráfico en una situación dada.

En el segundo mensaje (2), el receptor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación.

En el tercer (3) y cuarto (4) mensaje, el emisor y el receptor, respectivamente intercambian material clave usado para llegar a un secreto común compartido y la información aleatoria que es usada para garantizar la vida de la conexión y proteger contra ataques de reenvío.

En el quinto (5) y sexto (6) mensaje, el emisor y el receptor, respectivamente, intercambian información de identificación y los resultados de la función de autentificación acordada. Esta información es trasmitida bajo la protección de un secreto común compartido.

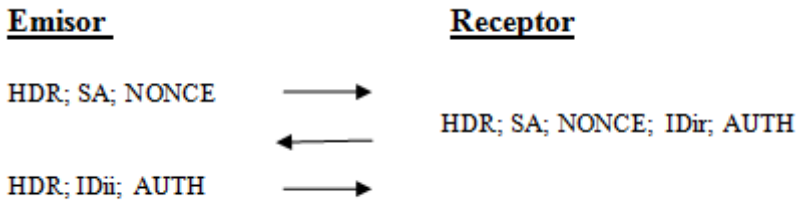
Intercambio de Autentificación

El Intercambio de Autentificación está diseñado para permitir solamente la Autentificación relacionada con la información a trasmitir.

El beneficio de este intercambio es la capacidad de realizar solamente la autentificación sin otro costo computacional de claves.

Usando este intercambio durante la negociación, ninguna información trasmitida será encriptada. Sin embargo, la información puede ser encriptada en otros lugares.

El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio de Autentificación.



En el primer mensaje (1), el emisor genera una propuesta que considera adecuada para proteger el tráfico en una situación dada. Las cargas, SA, la de la Propuesta, y la de Transformación, son incluidas en la carga SA (para simplificar la notación).

En el segundo (2) mensaje, el receptor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación.

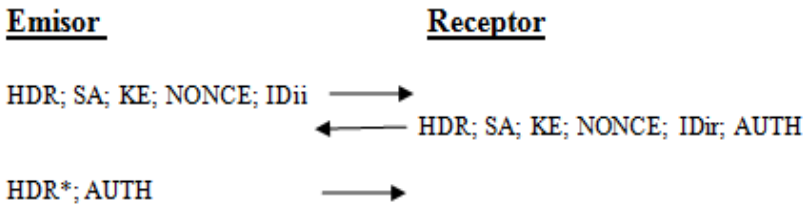
En el tercer (3) mensaje, el emisor trasmite la información de identificación. Esta información es trasmitida bajo la protección de una función de autentificación acordada.

Intercambio Agresivo

El Intercambio Agresivo está diseñado para permitir que la SA, el Intercambio de Claves y las cargas relacionadas con la Autentificación sean trasmitidas en forma simultánea. Combinar la SA, el intercambio de claves, y la información

relacionada con la Autentificación en un mensaje, reduce el número de viajes de ida y vuelta a expensas de no proporcionar la protección de identidad

El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio Agresivo.



En el primer mensaje (1), el emisor genera una propuesta que considera adecuada para proteger el tráfico para la situación dada. Las cargas, SA, la de la Propuesta, y la de Transformación, son incluidas en la carga SA (para simplificar la notación). Solamente puede existir una Propuesta y una Transformación ofrecida (es decir no hay elección) acordada para el funcionamiento del intercambio agresivo.

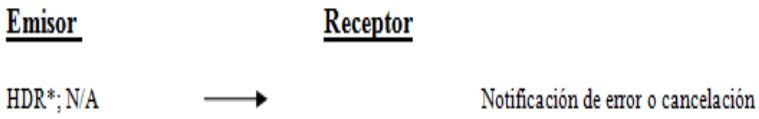
En el segundo (2) mensaje, el receptor indica el conjunto de protección que ha aceptado con las cargas, SA, la de la Propuesta, y la de Transformación.

En el tercer (3) mensaje, el emisor trasmite los resultados de la función de autentificación acordada. Esta información es trasmitida bajo la protección de un secreto común compartido

Intercambio Informativo

El Intercambio Informativo está diseñado como una transmisión unidireccional de información que puede ser usada para la administración de SA.

El siguiente diagrama muestra los mensajes con las posibles cargas enviadas en cada mensaje y las notas de ejemplo de un Intercambio Informativo.



En el primer mensaje (1), el emisor o el receptor transmite una Notificación ISAKMP o una carga de Cancelación.

3.5 LISTAS DE ACCESO (ACL)

Una Lista de Control de Acceso es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido. Listas de acceso permiten el filtrado basado en las direcciones de origen y destino, de entrada y salida a las interfaces específicas

Las ACLs permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico, permitiendo o denegando el tráfico de red de acuerdo a alguna condición. Sin embargo, también tienen usos adicionales, como por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión).

ACLs se usan para aplicar una política de seguridad que permite o niega el acceso de cierta parte de la red a otra. La granularidad de las ACLs permite que estas partes sean o bien PC específicos o partes de una subred arbitrariamente, es decir, permite que se conceda o niegue el acceso desde un único PC hasta otro, de un segmento de red a otro o cualquier combinación que se quiera.

También sirven para clasificar conjuntos de direcciones, por ejemplo una subred o una parte de una subred.

Las lista de acceso se identificada con un número o un nombre y todas las reglas que tengan el mismo número/nombre hacen parte de la ACL, éstos identificadores

suelen indicar también qué tanta expresividad tendrá la ACL, es decir, qué tan específicas pueden ser las reglas.

Un ejemplo de cómo es conceptualmente una ACL es así

- Lista-de-acceso X ACCION1 CONDICION1
- Lista-de-acceso X ACCION2 CONDICION2
- Lista-de-acceso X ACCION3 CONDICION3

La X es el nombre o número que identifica la ACL, por lo tanto todas las reglas anteriores componen la ACL X, o una sola. Si cierto paquete cumple la condición1 se le aplica la Acción1, si un paquete cumple la condición 2 se le aplica la acción 2 y así sucesivamente. Las acciones son sólo permitir o denegar y las condiciones dependen del tipo de ACL, las más simples, las estándar especifican valores para comparar con la dirección IP origen de cada paquete, en las más expresivas, llamadas extendidas, las condiciones permiten especificar valores para comparar tanto con la dirección IP origen como con la IP destino e incluso protocolos de capa 4 y parámetros de capa 4 como puertos y banderas de la conexión TCP.

La lógica de funcionamiento de las ACLs es que una vez que se cumpla una condición, se aplica su acción correspondiente y no se examinan más reglas de la ACL.

Estructura Básica

Las reglas que componen las listas de acceso tienen tres partes: un número que identifica la lista, una instrucción deny o permit y una condición

(access-list) (número_identificador (permit/deny)) (condición)

Ejemplo: access-list 1 permit 192.168.1.0 0.0.0.255

El número utilizado para identificar una lista concreta debe ser seleccionado de un rango numérico acorde con el uso concreto de la lista.

En la siguiente tabla 3.5-10 se muestran los principales tipos de listas disponibles.

PROTOCOLO	TIPO	RANGO	FILTRAR POR
IPv6	Estándar	1-99	El Origen
IPv6	Extendidas	100-199	El Origen, Destino, Protocolo, Puerto
Ethernet	Código	200-299	El Tipo de Código Ethernet

Tabla 3.5-10 Listas de Acceso disponibles

Autor: Investigador
Fuente: http://antonio_gallego.tripod.com/apuntes/listas.htm

Listas de Acceso en IPv6 tiene la misma función que IPv4, pero permite la configuración de línea de comandos, se utiliza para filtrar las conexiones entrantes y salientes desde y hacia un router basado en una lista de acceso IPv6 y solo se puede realizar de forma extendida.

Estructura: ipv6 access-list (name)

```
[no] permit | deny ipv6 | <protocol> any | host <src> |
src/len [sport] any | host <dest> | dest/len [dport] [reflect
<name> [timeout <secs>]] [fragments] [routing] [dscp
<val>] [flow-label <val>][time-range <name>] [log | log-
input] [sequence <num>]
```

Ejemplo: ipv6 access-list nom_uno
permit ipv6 2001:AAAA:1234:1::2/64 2001:AAAA:1234:2::2/64

3.5.1 TIPOS DE LISTAS DE ACCESO

Lista de Acceso Estándar

Las ACL estándar especifican un sólo par dirección de referencia contra el que se comparan todos los paquetes que entren o salgan de la interfaz en la que se instale la ACL, en otras palabras, una ACL estándar filtra tráfico con base en la dirección IP origen de los paquetes. Estas ACL se crean en modo de configuración global con el comando access-list seguido de un número de 1 a 99 éstos rangos identifican que el tipo de ACL es estándar.

Cada regla debe tener el mismo número para pertenecer a la misma ACL, si el número cambia, la regla en particular pertenecerá a otra ACL. Luego de Access-

list <número> sigue la acción a ejecutar (permit o deny) y finalmente la condición que deben cumplir los paquetes para aplicarles la acción o continuar examinando más reglas. Las ACL estándar usan un sólo par dirección para especificar la condición que deben cumplir los paquetes para que se les aplique la acción permit o deny.

Estructura: Se escribe en el modo de configuración global

access-list (número) (deny | permit) (ip origen) (wildcard origen)

Ejemplo:
Bloquear toda la subred 172.17.3.0/24, excepto la máquina 172.17.3.10.

access-list **1** permit host 172.17.3.10
access-list 1 deny 172.17.3.0 0.0.0.255
access-list 1 permit any

Una vez realizado el tipo de acceso de lista estándar, se habilita en las interfaces para que el tráfico pueda pasar en la red

Ejemplo:

interface fas0/0
ip access-group **1** in (permite habilitar el tráfico entrante)

Lista de Acceso Extendida

Las listas de acceso extendidas permiten especificar hacia dónde se dirige el tráfico y con ésta característica, se puede bloquear o permitir un tráfico mucho más específico: sólo tráfico que proviene del host pero se dirige a una red en particular o a otro host en particular o sólo el tráfico de una red que se dirige a otra red. Se logra con el hecho de permitir comparar las direcciones destino de los paquetes con la ACL, no sólo las direcciones origen.

Las condiciones en las ACL estándar están compuestas por una dirección de referencia que determina qué bits de la dirección origen de los paquetes se deben comparar con la dirección de referencia, en cambio en las ACL extendidas se especifica dos pares de direcciones de referencia, un par para la dirección origen de los paquetes y otro par para la dirección destino de los mismos.

Las ACL extendidas son mucho más eficientes en el filtrado que las estándar, pero son mecanismos de clasificación de tráfico y direcciones y hay algunas aplicaciones que se corresponden mejor con las estándar que con las extendidas, por lo tanto se siguen usando de acuerdo al requerimiento del usuario tanto como las estándar como las extendidas. Estas ACL se crean con el comando access-list seguido de un número de 100 a 199 éstos rangos identifican que el tipo de ACL es extendidas en IPv4 o IPv6.

Un ACL IPv4 tiene la siguiente estructura:

access-list (número) (deny | permit) (protocolo) (ip origen) (wildcard origen) (ip destino) (wildcard destino)

Ejemplo:

access-list 100 deny ip 192.168.1.1 0.0.0.0 172.16.1.1 0.0.0.0
access-list 100 permit ip 192.168.1.1 0.0.0.0 0.0.0.0 255.255.255.255

Un ACL IPv6 tiene la siguiente estructura:

ipv6 access-list (name)

[no] permit | deny ipv6 | <protocol> any | host <src> | src/len [sport] any | host <dest> | dest/len [dport] [reflect <name> [timeout <secs>]] [fragments] [routing] [dscp <val>] [flow-label <val>][time-range <name>] [log | log-input] [sequence <num>]

Ejemplo:

Ipv6 access-list acl_out
permit udp host 2001:BAAA:1234:2::4 host 2001:BAAA:1234:2::3 eq 500
permit esp host 2001:BAAA:1234:2::4 host 2001:BAAA:1234:2::3

Una vez realizado el tipo de acceso de lista extendido, se habilita en las interfaces para que el tráfico pueda pasar en la red pero para IPv6 se habilita de la siguiente manera:

Ejemplo:

interface fas0/0
ipv6 traffic-filter acl_out in/out (permite habilitar el tráfico entrante o saliente)

En este capítulo esta detallada la información a base de las diferentes RFC, las mismas que serán explicadas en los Anexos los tipos de RFC que fueron aplicados en este capitulo

CAPITULO IV

4. IMPLEMENTACION Y PRUEBAS DE LOS PROTOCOLOS DE SEGURIDAD PARA IPv6

En este capítulo se detalla las configuraciones y pruebas realizadas de acuerdo a la investigación hecha en los capítulos anteriores de los protocolos IPSec, IKE, ISAKMP con sus respectivos algoritmos criptográficos que son esenciales para las seguridades de información.

4.1 DISEÑO FISICO IMPLEMENTADO

En la siguiente figura 4.1-44 se muestra el diseño físico real implementado en la red prototipo bajo la infraestructura de Cisco para las pruebas de los protocolos de seguridad IPSec, IKE, ISAKMP bajo IPv6.

FIG.4.1-44 Diseño Físico Implementado en Cisco

Autor: Investigador
Fuente: Resultado de la Investigación

4.2 DISEÑO LOGICO IMPLEMENTADO

Para el diseño lógico implementado se utiliza Routers Ciscos 2801 porque este tipo de router permite la facilidad de implementar diferentes IOS para el funcionamiento de los protocolos de seguridad como IPsec, algoritmos de seguridad DES, AES y se utilizan Hosts que trabajen con Windows XP Profesional se utiliza este tipo de características tanto en los Routers como en los Hosts de acuerdo a los requerimientos mínimos.

En la siguiente figura 4.2-45 se muestra el diseño que permite detallar el tipo de direcciones como las interfaces que se utilizó en la red. En el punto 4.4.4 se detalla las interfaces y protocolos de los routers con los que se va a trabajar en la red

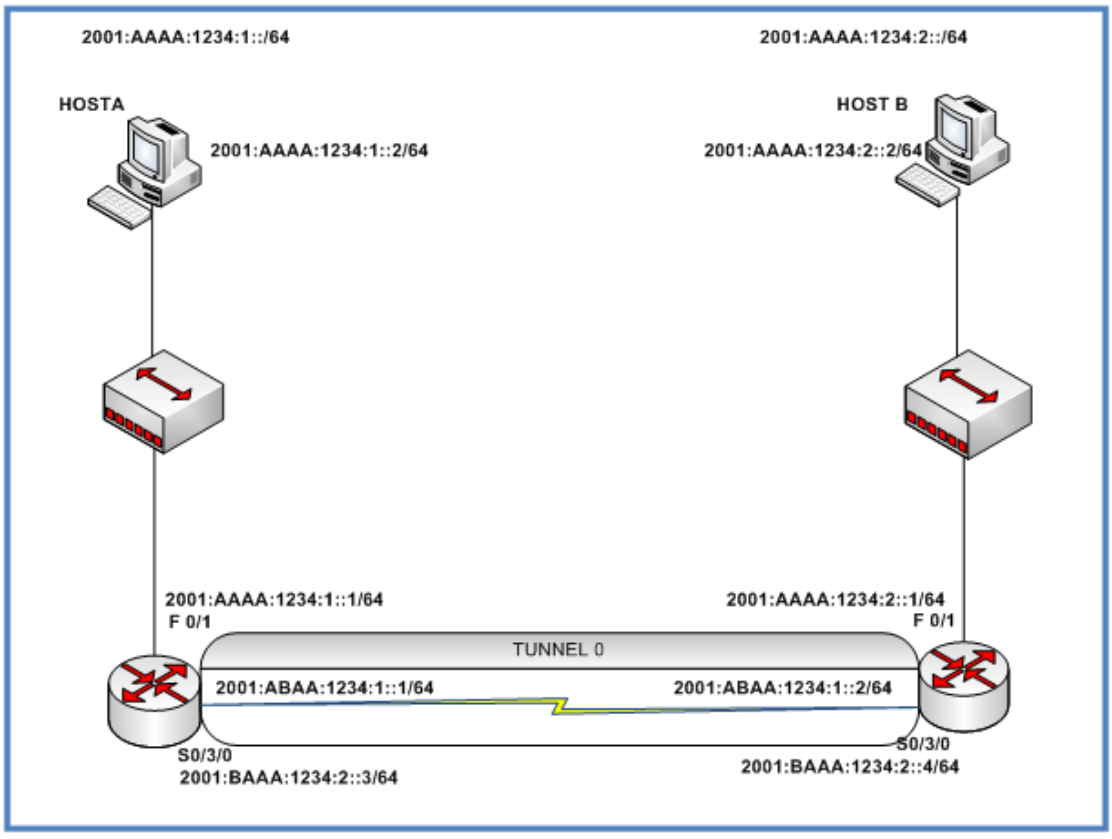


FIG.4.2-45 Diseño Lógico Implementado en Cisco

Autor: Investigador
Fuente: Resultado de la Investigación

Se puede utilizar Windows Vista, Windows 7, para el diseño lógico

4.3 REQUERIMIENTOS PARA LA RED

Para la implementación de la red es necesario conocer los tipos de requerimientos con los que se van a trabajar en cada equipo tanto en los Routers como en los diferentes Host.

4.3.1 REQUERIMIENTOS DE HARDWARE

Para la aplicación de seguridades de información en IPv6 se debe conocer los tipos de equipos que se van a usar en la red. En la siguiente tabla 4.3-11 se detalla las especificaciones y características de los equipos.

№	Equipo	Características
2	Hosts	- Windows XP Profesional - Pentium 4 - 160 GB de Disco Duro
2	Routers	- Cisco 2801 Serie - 64 MB Flash - 128 DRAM
2	Tarjetas de Red	- Ethernet 10/100 Mbps

Tabla.4.3-11 Requerimientos de Hardware de la Red

Fuente: Resultado de la Investigación

4.3.1.1 CARACTERISTICAS ESPECÍFICAS DEL ROUTER 2801

Es importante conocer las características del Router 2801 para que permita el funcionamiento de los diferentes protocolos de seguridad como IPSec y los algoritmos de seguridad DES, AES. De esta forma se tiene la seguridad que el tráfico que pasa por los Routers va a ser seguro y la información que se envía desde en emisor al receptor es confidencial.

Características Generales del Router

- Tipo de dispositivo: Encaminador

- Factor de forma: Externo - modular - 1U
- Dimensiones (Ancho x Profundidad x Altura): 43.8 cm x 41.9 cm x 4.5 cm
- Peso: 6.2 kg
- Memoria RAM: 128 MB (instalados) / 384 MB (máx.)
- Memoria Flash: 64 MB (instalados) / 128 MB (máx.)
- Protocolo de interconexión de datos: Ethernet, Fast Ethernet
- Red / Protocolo de transporte: IPSec
- Protocolo de gestión remota: SNMP 3
- Características: Cisco IOS , cifrado del hardware, soporte de MPLS
- Alimentación: CA 120/230 V (50/60 Hz)
- Requisitos del sistema: Microsoft Windows 98 Second Edition.

En la siguiente tabla 4.3-12 se detalla las características generales del router

General	
Tipo de dispositivo	Encaminador
Factor de forma	Externo - modular - 1U
Anchura	43.8 cm
Profundidad	41.9 cm
Altura	4.5 cm
Peso	6.2 kg

Memoria	
Memoria RAM	128 MB (instalados) / 384 MB (máx.)
Memoria Flash	64 MB (instalados) / 128 MB (máx.)

Conexión de redes	
Tecnología de conectividad	Cableado
Protocolo de interconexión de datos	Ethernet, Fast Ethernet
Red / Protocolo de transporte	IPSec
Protocolo de gestión remota	SNMP 3
Características	Cifrado del hardware, soporte de MPLS

Comunicaciones	
Tipo	DSU/CSU

Expansión / Conectividad	
Total ranuras de expansión (libres)	2 (2) x HWIC 2 (2) x AIM 2 (2) x PVDM 1 (1) x WIC 1 (1) x VIC 1 memoria 1 Tarjeta CompactFlash
Interfaces	2 x red - Ethernet 10Base-T/100Base-TX - RJ-45 1 x USB 1 x red - auxiliar 1 x gestión - consola

Diverso	
Algoritmo de cifrado	DES, Triple DES, AES
Cumplimiento de normas	CISPR 22 Class A, CISPR 24, EN 61000-3-2, VCCI Class A ITE, IEC 60950, EN 61000-3-3, EN55024, EN55022 Class A, UL 60950, EN50082-1, CSA 22.2 No. 60950, AS/NZ 3548 Class A, JATE, FCC Part 15, ICES-003 Class A, CS-03, EN 61000-6-2

Alimentación	
Dispositivo de alimentación	Fuente de alimentación - interna
Voltaje necesario	CA 120/230 V (50/60 Hz)

Software / Requisitos del sistema	
OS prorporcionado	Cisco IOS
Sistema operativo requerido	Microsoft Windows 98 Second Edition

Tabla 4.3-12 Características Generales del Router 2801

Autor: Investigador
Fuente:
http://www.cisco.com/application/pdf/en/us/guest/products/ps5854/c1616/ccmigration_09186a00802c35a2.pdf

4.3.2 REQUERIMIENTOS DE SOFTWARE

El software para la implementación práctica que se utiliza de acuerdo a los diferentes dispositivos de la investigación que se menciono en el punto anterior de este capítulo se mostrará en la siguiente tabla 4.3-13

Software	Descripción
Windows XP Professional	Sistema Operativo de los Hosts
Service Pack 2	Service Pack que ofrece soporte para IPv6
CISCO IOS Release 12.4 (11)T	Actualización de la versión del IOS del Cisco 2801 series, soporta IPv6.
Ethereal	Software de libre distribución, para la captura de tráfico de paquetes y análisis de protocolos de ruteo

Tabla.4.3-13 Requerimientos del Software de la Red

Fuente: Resultados de la Investigación

4.4 CONFIGURACION DE LOS EQUIPOS

En este punto del capítulo se detalla paso a paso las diferentes configuraciones que se realiza en los hosts y los routers, para el funcionamiento de la red bajo IPv6.

4.4.1 INSTALACION DE IPv6 EN PLATAFORMA WINDOWS XP

En general, las plataformas de Microsoft disponen de un buen soporte para IPv6. A partir de su versión de sistema operativo “Windows XP”, El protocolo viene preinstalado y su configuración es muy sencilla.

Se puede instalar IPv6 de dos formas:

- **Configuración de IPv6 en el Host**

  Para realizar la configuración de Ipv6 se realiza los siguientes pasos:

  1. Pulsar Inicio, luego Panel de Control, y luego hacer doble clic en Conexiones de red.
  2. Pulsar con el botón derecho en cualquier conexión de área local y luego Pulsar en Propiedades.

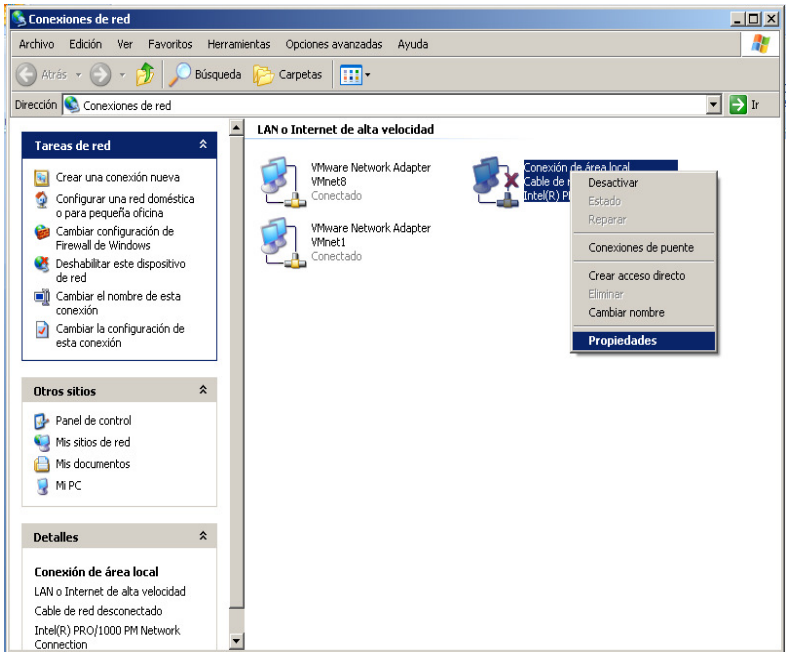


FIG.4.4-46 Conexión de Red

Fuente: Resultado de la Investigación

3. Dentro de Propiedades seleccionar Instalar

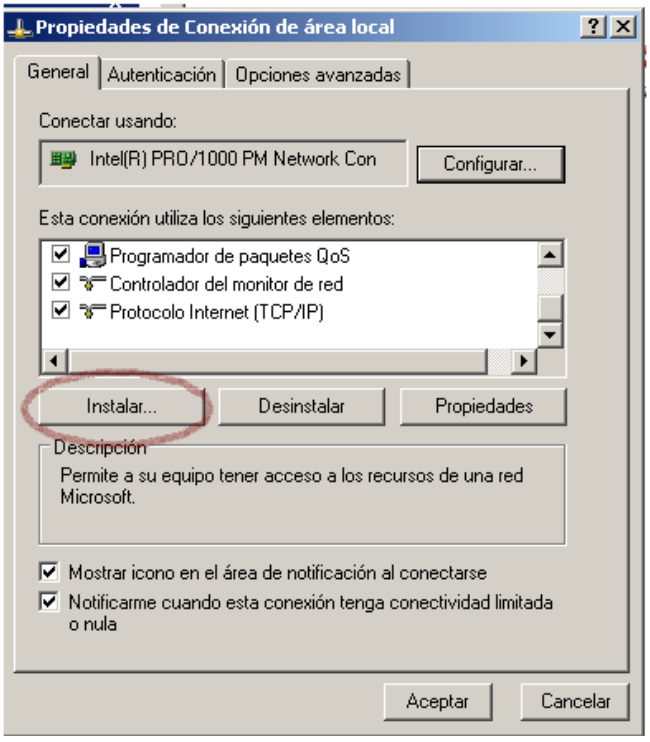


FIG.4.4-47 Propiedades de la Conexión de Red

Fuente: Resultado de la Investigación

4. Seleccionar Protocolo

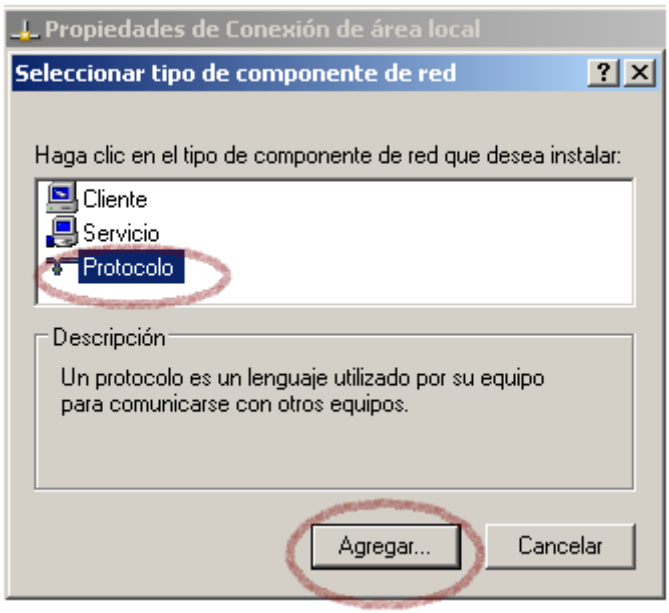


FIG.4.4-48 Tipo de Componente de Red

Fuente: Resultado de la Investigación

5. Seleccionar Ipv6

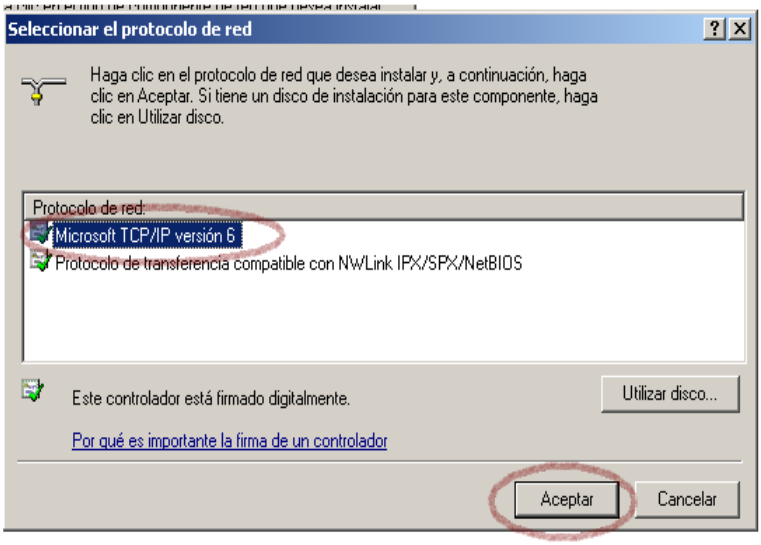


FIG.4.4-49 Protocolo de Red

Fuente: Resultado de la Investigación

6. Finalmente se ha instalado Ipv6 en el Host

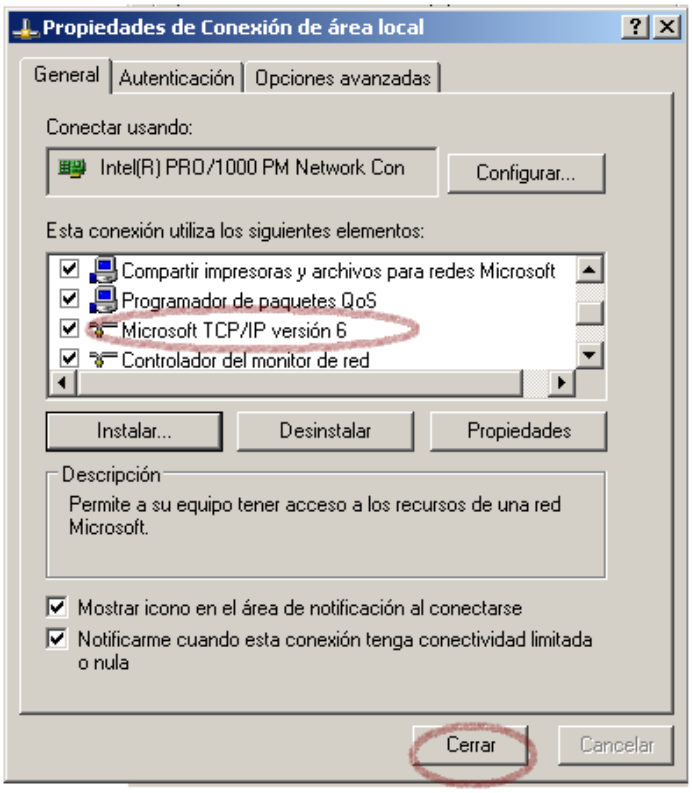


FIG.4.4-50 Instalación de IPv6

Fuente: Resultado de la Investigación

- **Configuración Manual de IPv6 en el Host**

  Para Habilitar Ipv6 de forma manual se debe seguir los siguientes pasos

1. Ingresar a Consola

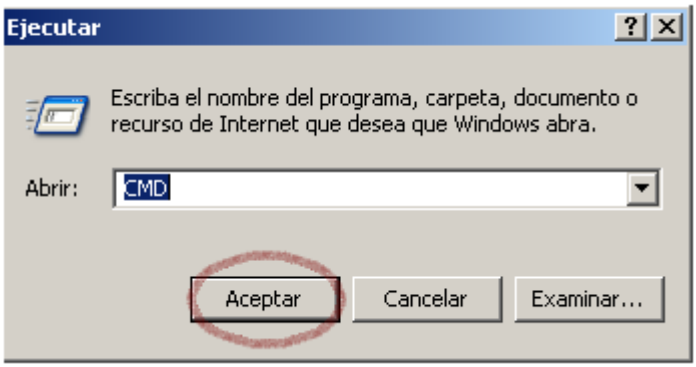


FIG.4.4-51 Ingreso a modo Consola

Fuente: Resultado de la Investigación

2. Instalar Ipv6 con el comando **ipv6 install**

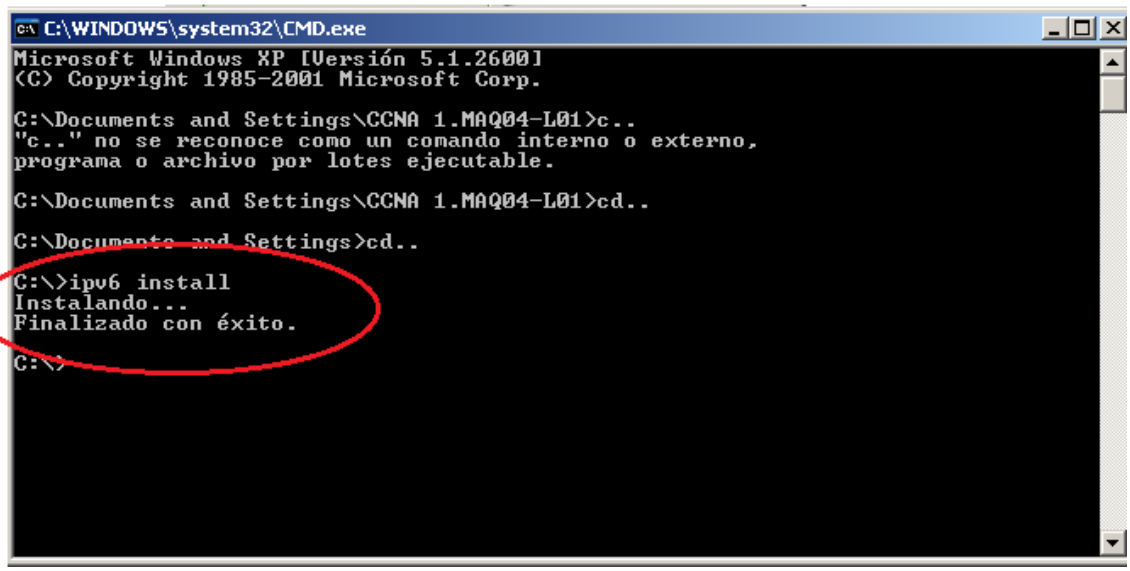


FIG.4.4-52 Instalación de IPv6 por Consola

Fuente: Resultado de la Investigación

4.4.2 INGRESO DE LA DIRECCION IPV6 EN EL HOST

En ausencia de router IPv6, se pueden configurar manualmente las direcciones IPv6 adicionales en las interfaces de red mediante el comando **netsh** interface **ipv6 add address**.

Este comando permite especificar la interfaz, la dirección, los tiempos de vida preferido y válido y si la dirección es unicast o anycast. Se debe tener en cuenta que las direcciones configuradas manualmente deben ser accesibles para poderse comunicar con otros nodos IPv6.

A continuación se muestra el formato de configuración de direcciones ipv6 y los métodos de comprobación de estado de las interfaces del host.

Parámetros

- Especifica un nombre de interfaz o índice:

  [[interface=] cadena]

- Requerido. Especifica la dirección IPv6 que se va a agregar.

  [address=] direcciónIPv6

- Especifica si se agrega una dirección de unidifusión (unicast) o una dirección de cualquier difusión. La opción predeterminada es unicast.

  [[*type*=]{ unicast| anycast}]

- Específica durante cuánto tiempo será válida la dirección. El valor predeterminado es infinite.

  [[validlifetime=]{entero| infinite}]

- Específica durante cuánto tiempo la dirección será la preferida. El valor predeterminado es infinite.

  [[preferredlifetime=]{entero| infinite}]

- Especifica si el cambio dura sólo hasta el próximo inicio (active) o si persistirá (persistent). La opción predeterminada es persistent.

  [[store=]{ active| persistent}]

A continuación se detalla los siguientes pasos para el ingreso de las direcciones de IPv6 manualmente en el host:

1. Pulsar I**nicio**, y seleccionar **Ejecutar.**

2. Se instala IPv6 manualmente como se detallo en el punto anterior.

3. Para saber con qué tipo de interfaz trabaja la máquina se ingresa el siguiente comando Ipv6 if.

   Es necesario conocer con qué tipo de interface está trabajando el hosts, debido que no todos los hosts tienen el mismo número de la interfaz. En la siguiente figura 4.4-53 se muestra la interfaz

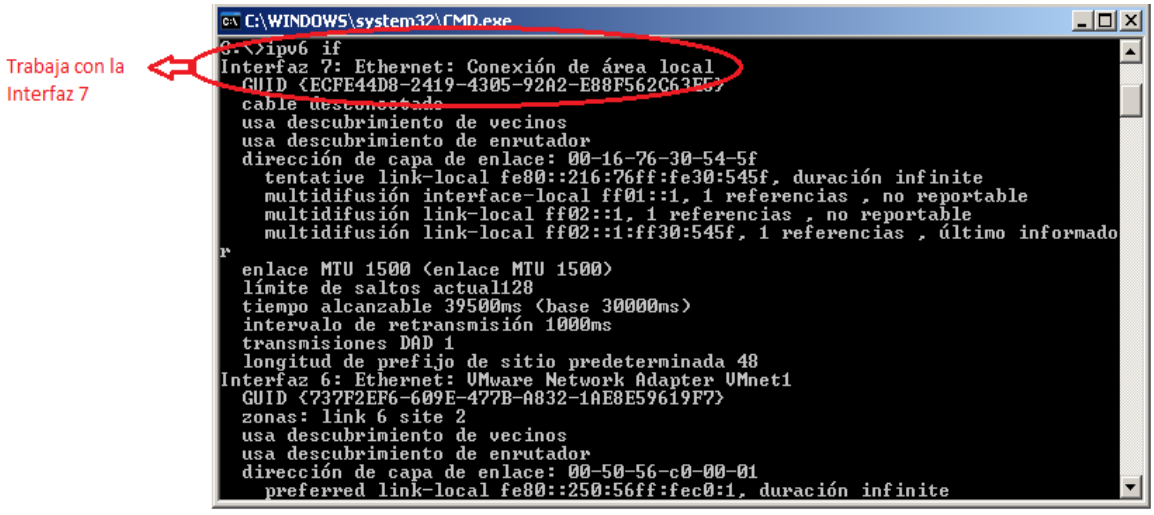


FIG.4.4-53 Tipo de Interfaz que trabaja el Host

Fuente: Resultado de la Investigación

4. Se comprueba el correcto funcionamiento de IPv6 mediante el comando **ping6 ::1** es la dirección de loopback en IPv6, al igual que 127.0.0.1 en IPv4.

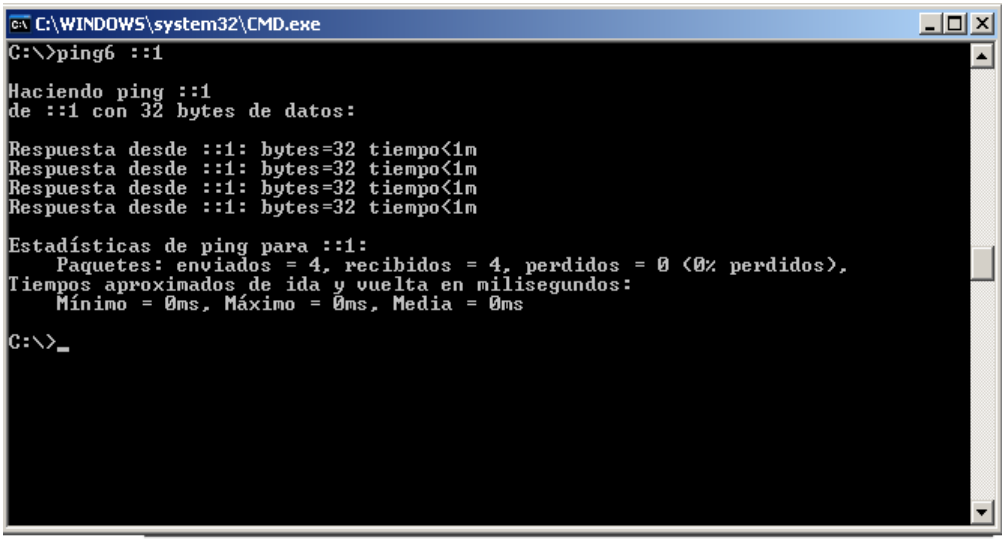


FIG.4.4-54 Dirección loopback IPv6

Fuente: Resultado de la Investigación

5. Ingresar la Dirección Ipv6 en el Host

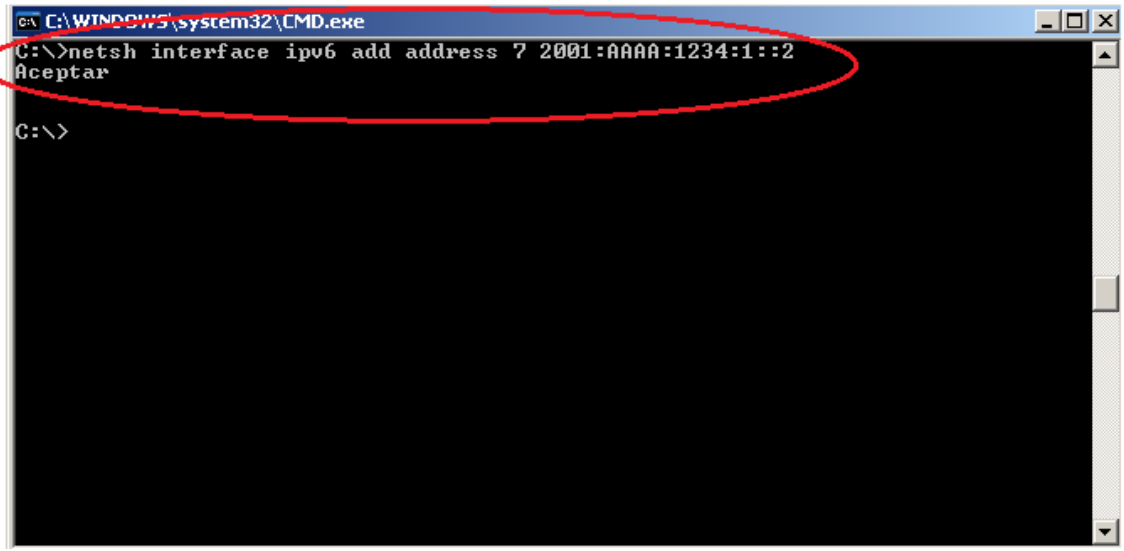


FIG.4.4-55 Dirección IPv6

Fuente: Resultado de la Investigación

De esta manera se ha ingresado la dirección IPv6 del Host. Si se ha cometido algún error en el proceso de configuración de la dirección IPV6, se usará este comando para proceder a eliminar la dirección errónea y con el procedimiento anteriormente descrito, volver a configurar la dirección correcta:

netsh interface ipv6 delete address 7 2001:AAAA:1234:1::2

4.4.3 CONEXION AL ROUTER CON DIRECCION IPv6

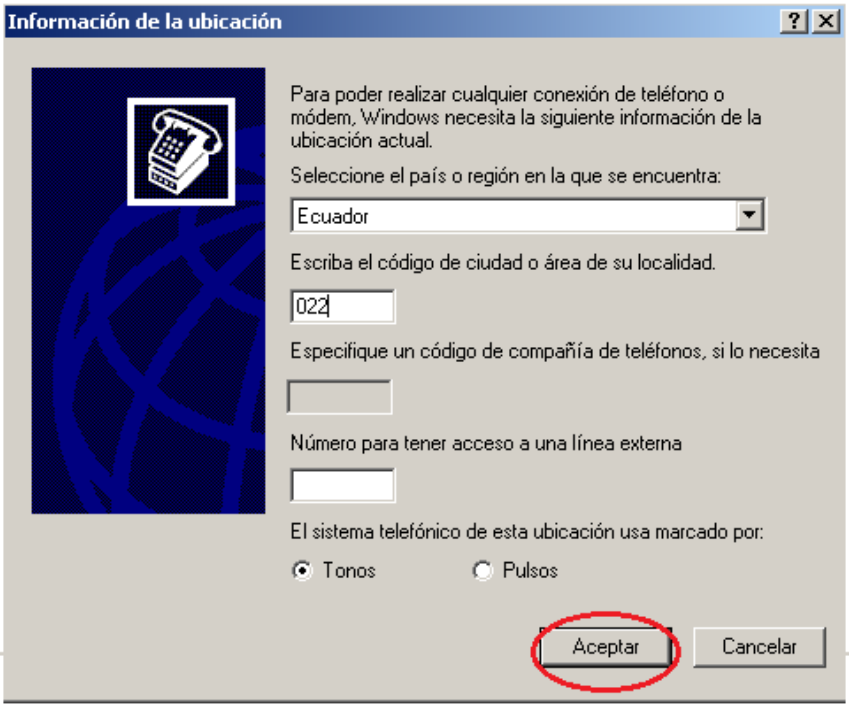
Para realizar la conexión al router se necesita ingresar por modo consola del router y seguir los siguientes pasos:

1. Ingresar Inicio, Programas, Accesorios y seleccionar Comunicación Hyperterminal.

FIG.4.4-56 Ingreso a Modo Consola al Router

Fuente: Resultado de la Investigación

2. Escribir el código de ciudad o región y Aceptar



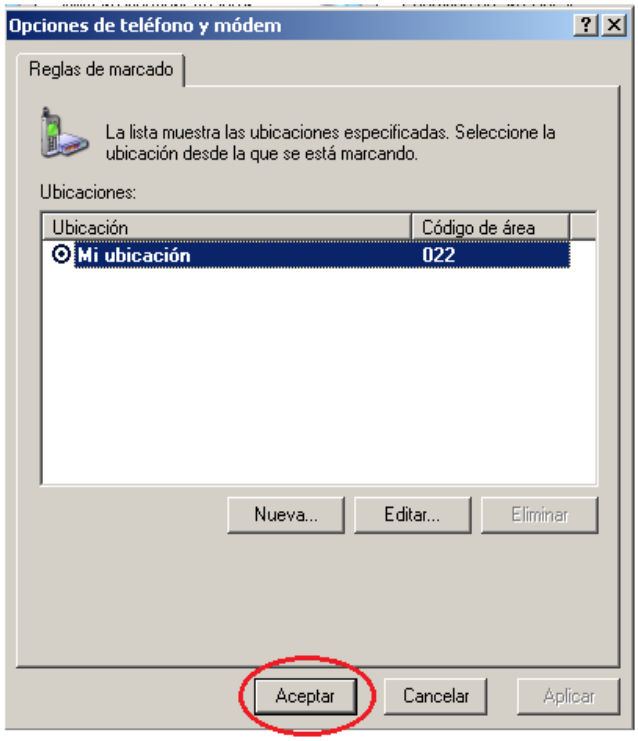


FIG.4.4-57 Información de Conexión

Fuente: Resultado de la Investigación

3. Escribir el Nombre y elegir el Icono para la conexión

FIG.4.4-58 Descripción de la Conexión

Fuente: Resultado de la Investigación

4. Seleccionar el puerto de comunicación para la conexión con el router que en este caso es el COM1 es el nombre que se le da al puerto serial, es una comunicación real con una apertura directa.

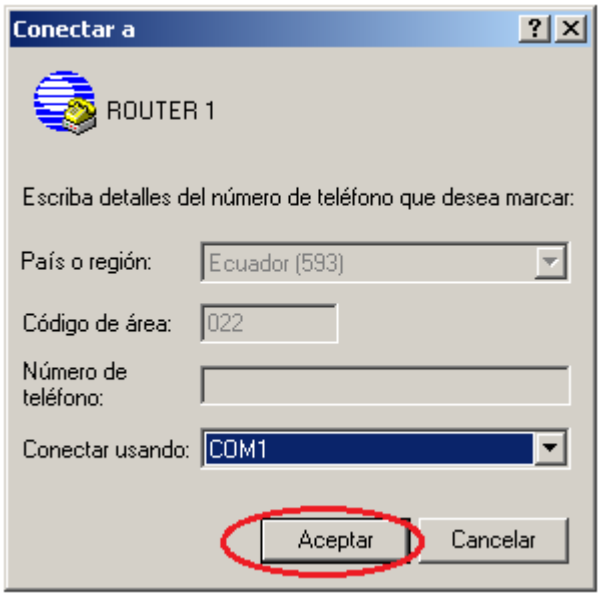


FIG.4.4-59 Selección del Puerto para la Comunicación

Fuente: Resultado de la Investigación

5. Configurar el puerto COM1 como se presenta en la figura 4.4-60

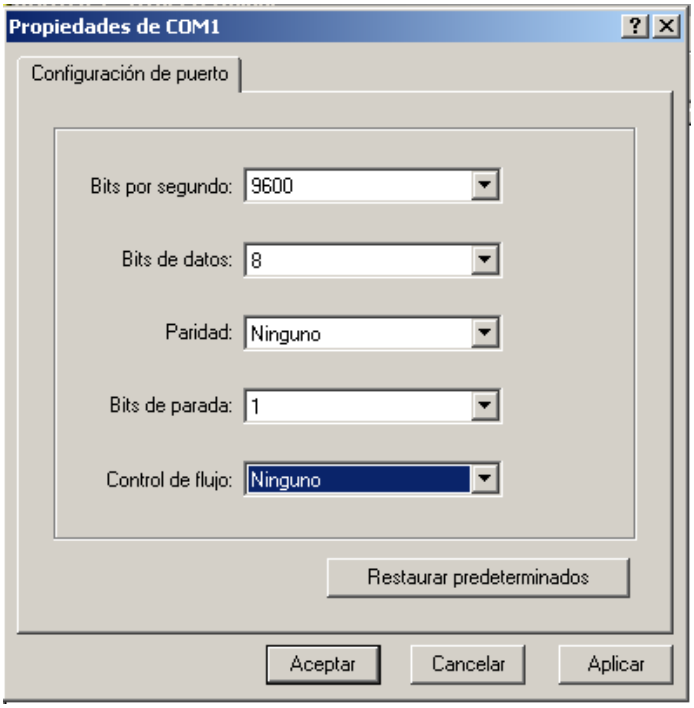


FIG.4.4-60 Configuración del Puerto COM1

Fuente: Resultado de la Investigación

Se configura el puerto de la conexión al router con las características anteriormente presentadas por las siguientes razones:

- **Bits por segundo**: Seteado a 9600 debido a la tasa de baudios que transmite el router.
- **Bits de datos:** Con valor 8, especifica los bits de datos para este puerto.
- **Paridad**: Seteada a ninguna, especifica la paridad para este puerto.
- **Bits de parada**: Seteada a 1 especificando la tasa de baudios para este puerto.
- **Control de flujo**: Seteado por hardware. En realidad no se requiere control de flujo debido a que los routers cisco trabajan a la misma velocidad

6. Se procede a encender el Router y se establecerá la comunicación, mostrando la configuración de inicio como se ve en la siguiente figura 4.4-61, donde las IOS que se está levantando correctamente

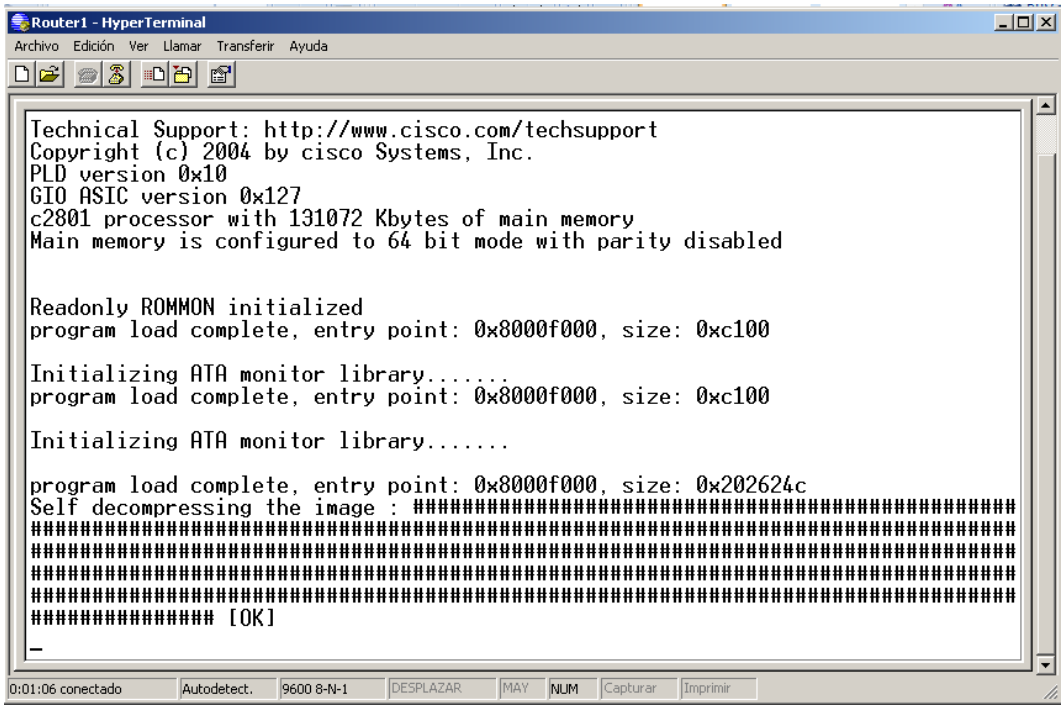


FIG.4.4-61 Router esta encendido

Fuente: Resultado de la Investigación

4.4.4 CONFIGURACION DE LAS INTERFACES Y PROTOCOLOS DEL ROUTER

Una vez realizada la conexión del router y este encendido, se procederá a la configuración de las interfaces y protocolos con los que se va a trabajar en la red de acuerdo al diseño lógico implementado en la red. En la Tabla 4.4-14 se muestra los requisitos necesarios para las configuraciones de los routers.

DESCRIPCION	HOST A	HOST B	ROUTER A	ROUTER B
Nombre de los Equipos	HOSTA	HOST B	Router 1	Router 2
Contraseña de Consola	No asignada	No asignada	cisco	cisco
Contraseña VTY	No asignada	No asignada	cisco	Cisco
Dirección IPv6 Fas 0/1	2001:AAAA:1234:1::2/64	2001:AAAA:1234:2::2/64	2001:AAAA:1234:1::1/64	2001:AAAA:1234:2::1/64
Dirección IIPv6 Ser 0/3/0	No asignada	No asignada	2001:BAAA:1234:2::3/64	2001:BAAA:1234:2::4/64
Dirección IPv6 Tunnel0	No asignada	No asignada	2001:ABAA:1234:1::1/64	2001:ABAA:1234:1::2/64
Rutas Estáticas	No asignada	No asignada	SI	SI
Protocolos de Seguridad	No asignada	No asignada	IPSEC, IKE,ISAKMP	IPSEC, IKE,ISAKMP
Activar Interfaces	SI	SI	SI	SI

Tabla 4.4-14 Requisitos de Configuración

Fuente: Resultados de la Investigación

4.4.4.1 CONFIGURACION DE LAS INTERFACES

En este punto se asignará las direcciones IPv6 a las interfaces de los Routers de forma individual de acuerdo a la tabla 4.4-14 y al diseño lógico.

A continuación se realizará los siguientes pasos para la configuración de las interfaces y las rutas estáticas de los routers para la conexión entre ellos.

Para ingresar a las interfaces o las criptografías se debe realizar los siguientes pasos que son esenciales en los routers:

- **Enable:** Se ingresa en modo privilegiado EXEC
- **Configure terminal:** Se ingresa al modo de configuración global

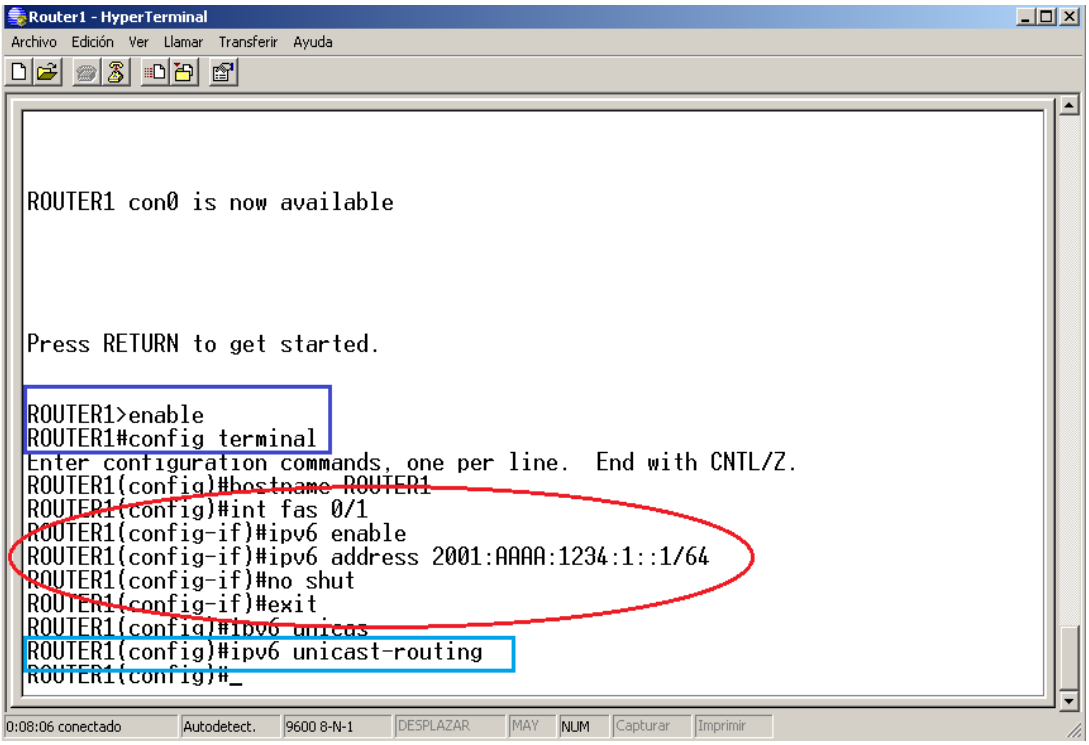
4.4.4.1.1 INTERFACE FAST ETHERNET

ROUTER 1

```
interface fastethernet 0/1      // especifica la interface donde se va a  implementar la configuración//
ipv6 enable                     // activa el protocolo IPv6//
ipv6 address 2001:AAAA:1234:1::1/64  //asigna una dirección ipv6 a la interface//
no shutdown                     // activa el protocolo IPv6//
exit                            // sale del modo de configuración anterior//
ipv6 unicast-routing            //Activa el reenvío de paquetes IPv6 en modo Unicast //
```

ROUTER 2

```
interface fastethernet 0/1      // especifica la interface donde se va a  implementar la configuración//
ipv6 enable                     // activa el protocolo IPv6//
ipv6 address 2001:AAAA:1234:2::1/64  //asigna una dirección ipv6 a la interface//
no shutdown                     // activa el protocolo IPv6//
exit                            // sale del modo de configuración anterior//
ipv6 unicast-routing            //Activa el reenvío de paquetes IPv6 en modo Unicast //
```



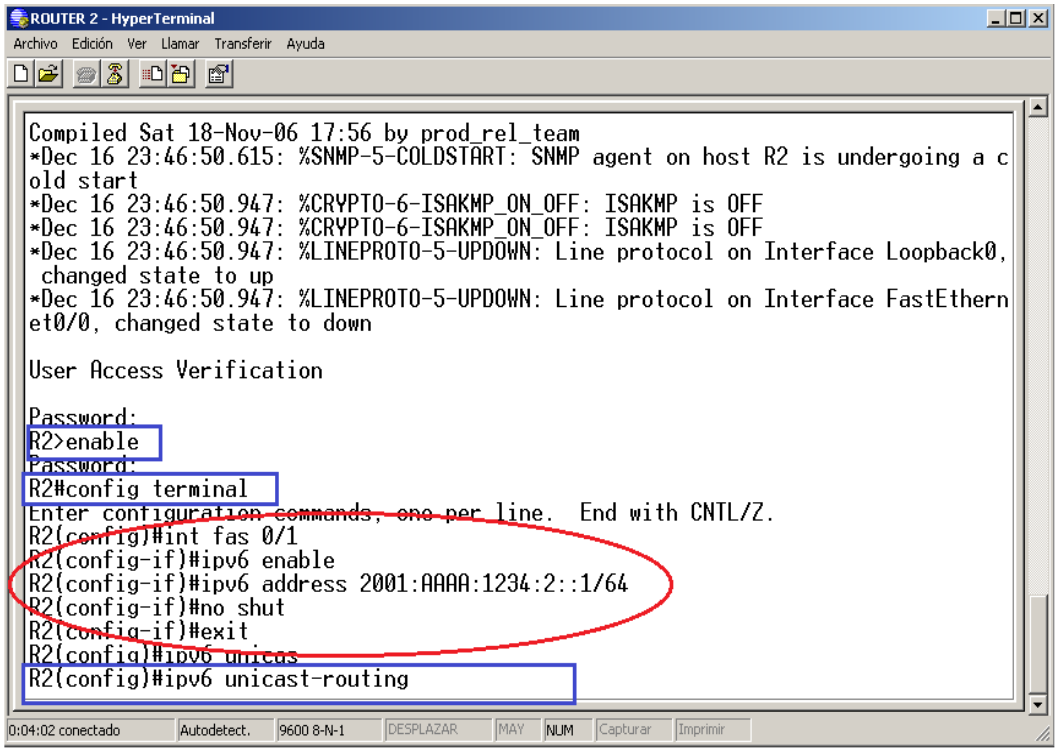


FIG.4.4-62 Comandos de la Interface FAS 0/1 (Router 1, 2)

Fuente: Resultado de la Investigación

4.4.4.1.2 INTERFACE SERIAL

ROUTER 1

interface serial 0/3/0 // especifica la interface donde se va a implementar la configuración//

ipv6 enable // activa el protocolo IPv6//

ipv6 address 2001:BAAA:1234:2::3/64 //asigna una dirección ipv6 a la interface//

R1 es el lado DCE de la conexión serial. DCE significa Data Controller Equipment o Equipo Controlador de Datos, Este router es el encargado de sincronizar el enlace punto a punto o es el encargado de configurar el ancho de banda que se le dará al lado DTE (Equipo Terminal de Datos) en el Router 2

clock rate 64000 //Valor de la velocidad del DCE. Se elije 64000 porque será la cantidad de bits que se pueda enviar en un momento dado, después de esta cantidad no se podrá enviar más rápido que 64000 a través de la red a menos que se cambie el valor//

no shutdown // activa el protocolo IPv6//

exit // sale del modo de configuración anterior//

ipv6 unicast-routing //Activa el reenvío de paquetes IPv6 en modo Unicast //

ROUTER 2

interface serial 0/3/0 // especifica la interface donde se va a implementar la configuración//

ipv6 enable // activa el protocolo IPv6//

ipv6 address 2001:BAAA:1234:2::4/64 //asigna una dirección ipv6 a la interface//

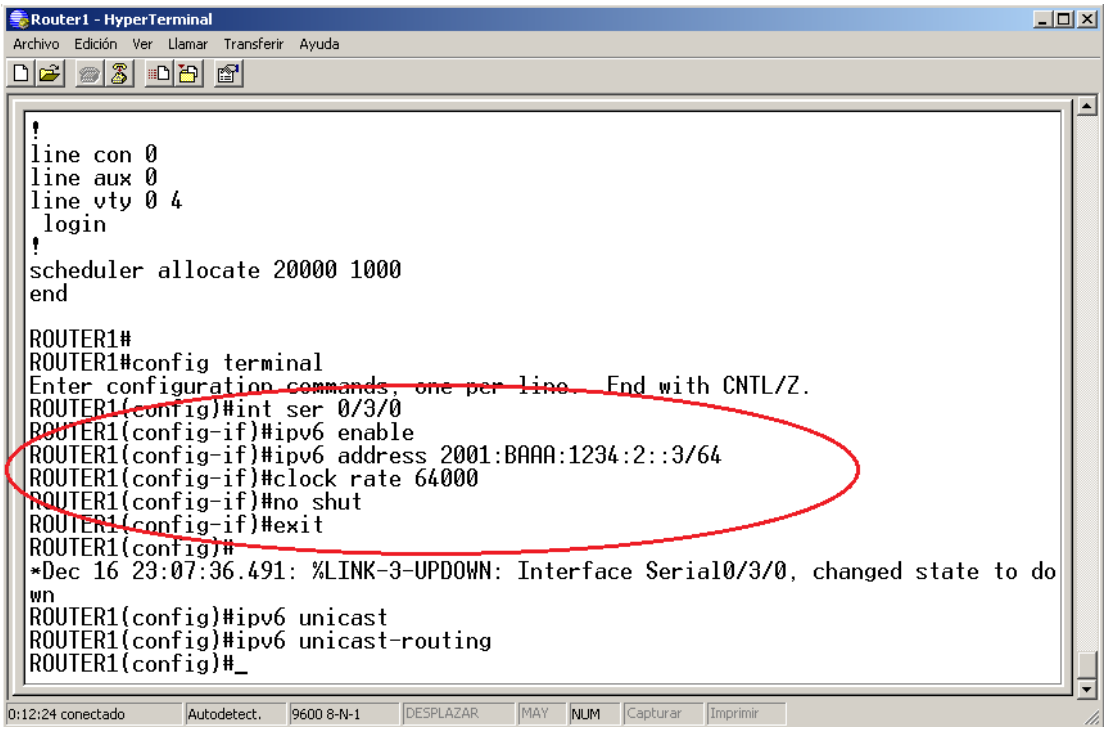
no shutdown // activa el protocolo IPv6//

exit // sale del modo de configuración anterior//

ipv6 unicast-routing //Activa el reenvío de paquetes IPv6 en modo Unicast //

Clock rate se activar en el Router que tenga el lado DCE, pero si se configura el clock rate en el lado DTE, este no tendrá ningún efecto en la sincronización del enlace, ya que DCE es quien controla la Velocidad de la Transmisión. Si se

setean 64Kbps en el DCE y 2Mbps en el DTE, el enlace funcionara a 64Kbps. Es por esta razón que DCE se configura por lo general en el lado del proveedor de Internet (ISP)



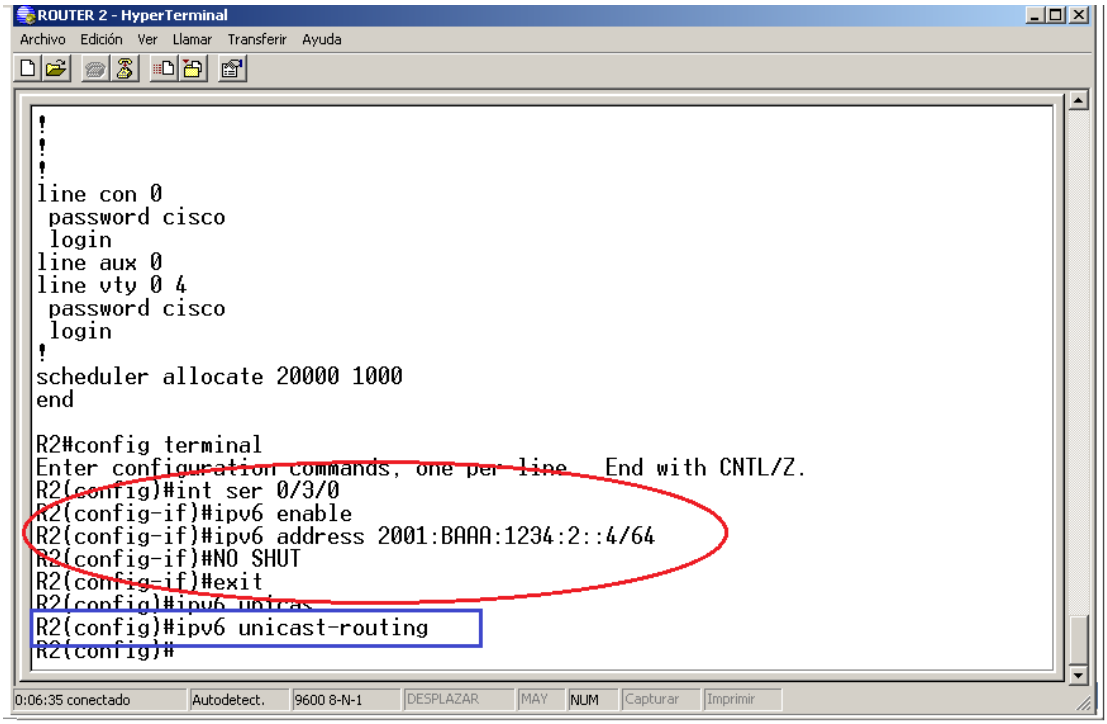


FIG.4.4-63 Comandos de la Interface Serial 0/3/0 (Router 1, 2)

Fuente: Resultado de la Investigación

4.4.5 IMPLEMENTACION DE RUTAS ESTATICAS

Las rutas estáticas permiten establecer la comunicación de extremo a extremo de la red, se utiliza este tipo de ruta porque específicamente indica al enrutador que ruta tomar para enviar ciertos paquetes.

Es seguro, dado que sólo las rutas especificadas van a ser utilizadas y no requiere ningún ancho de banda para enviar actualizaciones de rutas. Se definen administrativamente y establecen rutas específicas para que los paquetes puedan pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador.

Las rutas estáticas por default especifican un gateway (puerta de enlace) de último recurso, a la que el router debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir que desconoce. Las desventajas de usar este tipo de ruta es requerir la actualización manual cada vez que la red cambia de nivel IP como añadir manualmente cada red en cada equipo

Se utiliza este tipo de ruta porque se realiza habitualmente en enrutamientos desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento.

Sintaxis

ipv6 route <prefijo_IPv6>/<longitud_del_prefijo> <interfaz_o_gateway>
ipv6 route X:X:X:X::X/<0-128> IPv6 prefix x:x::y/<z>

nota: en caso de querer usar un gateway por defecto:
prefijo_IPv6/longitud_del_prefijo= :: /0

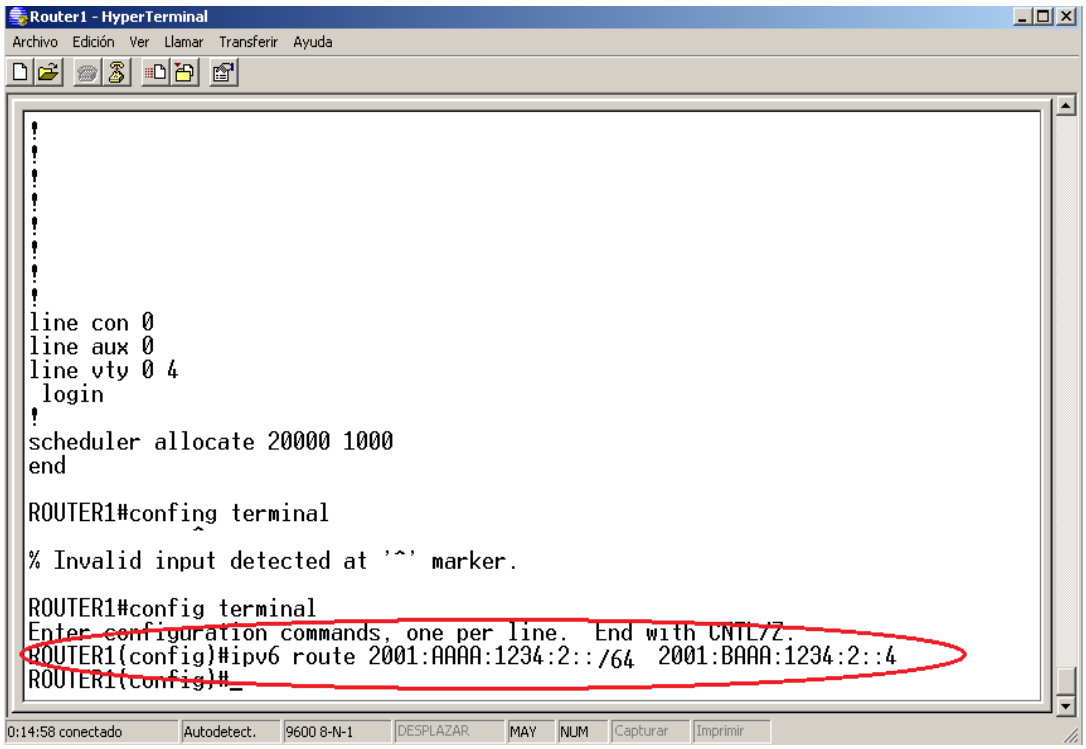
ROUTER 1

Router 1 (config)#ipv6 route 2001:AAAA:1234:2::/64 2001:BAAA:1234:2::4
//asigna una dirección ipv6 de la Red B y la dirección ipv6 de la interfaz serial del Router 2//

ROUTER 2

Router 1 (config)#ipv6 route 2001:AAAA:1234:1::2/64 2001:BAAA:1234:2::3

//asigna una dirección ipv6 de la Red A y la dirección ipv6 de la interfaz serial del Router 1//



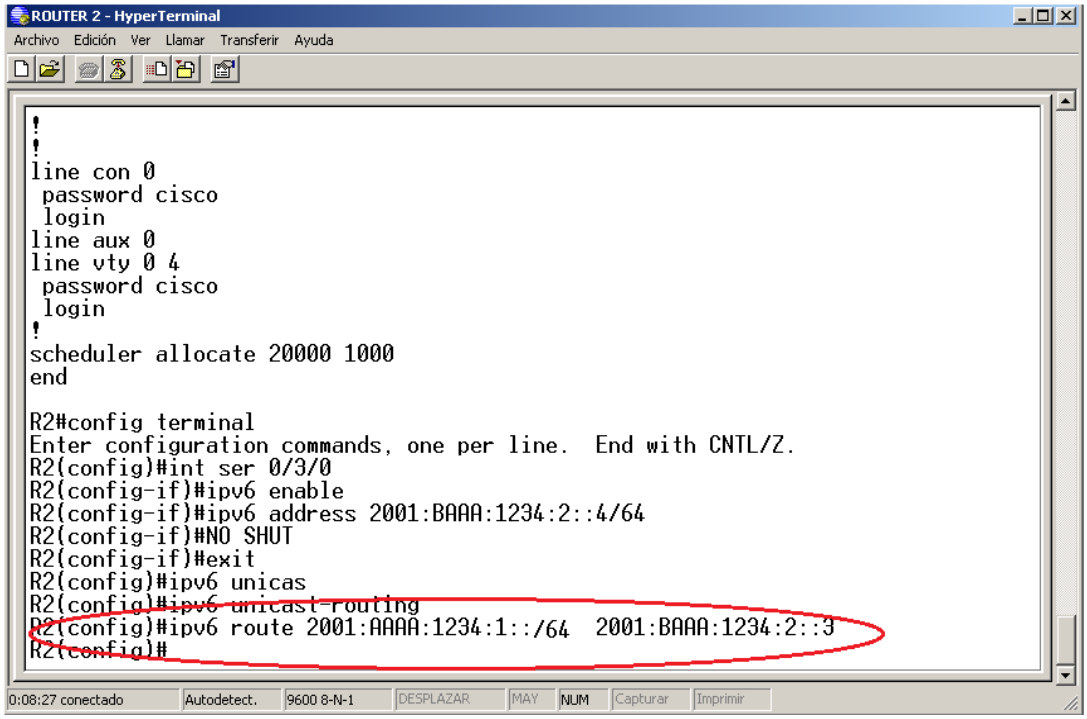


FIG.4.4-64 Implementación de Rutas Estáticas (Router 1, 2)

Fuente: Resultado de la Investigación

4.4.6 POLITICAS DE NEGOCIACION DEL PROTOCOLO IKE

Para configurar las políticas de IKE se define una combinación de parámetros de seguridad que serán usados durante la negociación IKE. En ambos nodos deben crearse políticas y al menos debe existir una igualdad en los 2 extremos.

Es un protocolo que define el método de intercambio de claves sobre IP en una primera Fase de negociación segura y la Fase segunda se negocian las SAs que requieren servicios como IPsec

4.4.6.1 FASE I

La Fase I del protocolo IKE se define las seguridades a través de la Autentificación, Encriptación que se generan en ISAKMP. En el siguiente punto se detalla la sintaxis de la implementación.

FASE 1

Parámetro	Fuerte	Mas Fuerte
Algoritmo de Cifrado por Bloques	DES (56 bits) 3DES (168 bits)	AES (128/256 bits)
Algoritmo Hash	MD5 (HMAC)	SHA-1 (HMAC)
Método de Autentificación	Pre-Share	+ Cifrado (RSA)
Intercambio de llaves	Diffie-Hellman Grupo 1 (768 bits)	Diffie-Hellman Grupo 2 (1024 bits)
Tiempo de Vida IKE	<86400 seg	86400 seg

Tabla 4.4-15 Fase 1 del protocolo IKE

Fuente: Resultados de la Investigación

4.4.6.1.1. IMPLEMENTACION DEL PROTOCOLO ISAKMP

ROUTER 1

crypto isakmp enable //Habilita IKE de manera global en todas las interfaces del router//

Cada política se identifica por su número de prioridad (1-10000) siendo 1 la prioridad más alta. En este caso la prioridad será 10 para ordenar la aplicación de las políticas de encriptación

crypto isakmp policy 10 //Crea una política IKE (política de encriptación de IKE) //

Método de autentificación para el intercambio de claves. Puede ser RSA, RSA encriptados y claves pre-configuradas, (las dos primeras necesitan un servidor de autoridad)

authentication pre-share //Especifica el algoritmo de autentificación dentro de la política IKE, se elije pre-share porque las claves son pre-configuradas //

encryption aes //Especifica el método de encriptación o cifrado dentro de la política IKE, Se elije AES porque es un algoritmo más seguro de 128/256 bits//

Hash es un algoritmo que permite generar un valor de resumen de algunos datos como una clave de mensaje o sesión, Con buen algoritmo de hash los cambios que se produzcan, puede cambiar a todos los bits. MD5 necesita configurarla en cambio SHA-1 no necesita.

hash md5 //Especifica el algoritmo hash a usar, se elegí MD5 porque es un algoritmo de reducción criptográfico de 128 bits //

Diffie-Hellman se utilizan para determinar la longitud del material clave, utilizado durante el proceso de intercambio de claves

group 2 //Especifica el identificador de grupo Diffie-Hellman, se elije el grupo 2 que es 1024 bits más fuerte que el grupo 1//

exit //Vuelve al modo de configuración global//

Se define una clave secreta que se usara desde un router a otro, y como se eligió claves pre-configuradas (PRE-SHARE, AES, MD5) que se intercambian en la negociación inicial es necesario configurarlas en cada extremo, para lo cual se utiliza el siguiente comando:

crypto isakmp key CLAVE address PEER-ADDRESS

crypto isakmp key cisco1234 address ipv6 2001:BAAA:1234:2::4/64

//Configuración de la llave para la autentificación pre-compartida, se elije el peer-address a la dirección de la interfaz serial 0/3/0 del router 2//

ROUTER 2

crypto isakmp enable //Habilita IKE de manera global en todas las interfaces del router//

Cada política se identifica por su número de prioridad (1-10000) siendo 1 la prioridad más alta. En este caso la prioridad será 10 para ordenar la aplicación de las políticas de encriptación

crypto isakmp policy 10 //Crea una política IKE (política de encriptación de IKE) //

Método de autentificación para el intercambio de claves. Puede ser RSA, RSA encriptados y claves pre-configuradas, (las dos primeras necesitan un servidor de autoridad)

authentication pre-share //Especifica el algoritmo de autentificación dentro de la política IKE, se elije pre-share porque las claves son pre-configuradas //

encryption aes //Especifica el método de encriptación o cifrado dentro de la política IKE, Se elije AES porque es un algoritmo más seguro de 128/256 bits//

Hash es un algoritmo que permite generar un valor de resumen de algunos datos como una clave de mensaje o sesión, Con buen algoritmo de hash los cambios que se produzcan, puede cambiar a todos los bits. MD5 necesita configurarla en cambio SHA-1 no necesita.

hash md5 //Especifica el algoritmo hash a usar, se elege MD5 porque es un algoritmo de reducción criptográfico de 128 bits //

Diffie-Hellman se utilizan para determinar la longitud del material clave, utilizado durante el proceso de intercambio de claves

group 2 //Especifica el identificador de grupo Diffie-Hellman, se elije el grupo 2 que es 1024 bits más fuerte que el grupo 1//

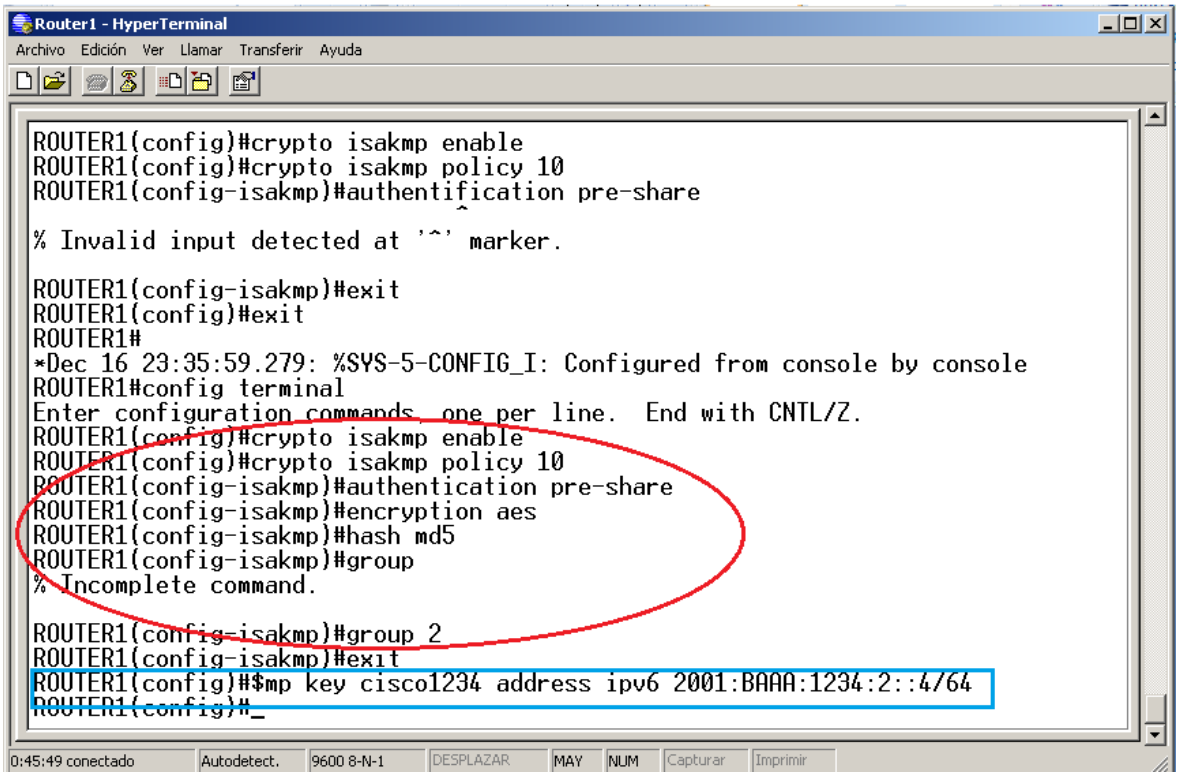
exit //Vuelve al modo de configuración global//

Se define una clave secreta que se usara desde un router a otro, y como se eligió claves pre-configuradas (PRE-SHARE, AES, MD5) que se intercambian en la negociación inicial es necesario configurarlas en cada extremo, para lo cual se utiliza el siguiente comando:

crypto isakmp key CLAVE address PEER-ADDRESS

crypto isakmp key cisco1234 address ipv6 2001:BAAA:1234:2::3/64

//Configuración de la llave para la autentificación pre-compartida, se elije el peer-address a la dirección de la interfaz serial 0/3/0 del router 1//



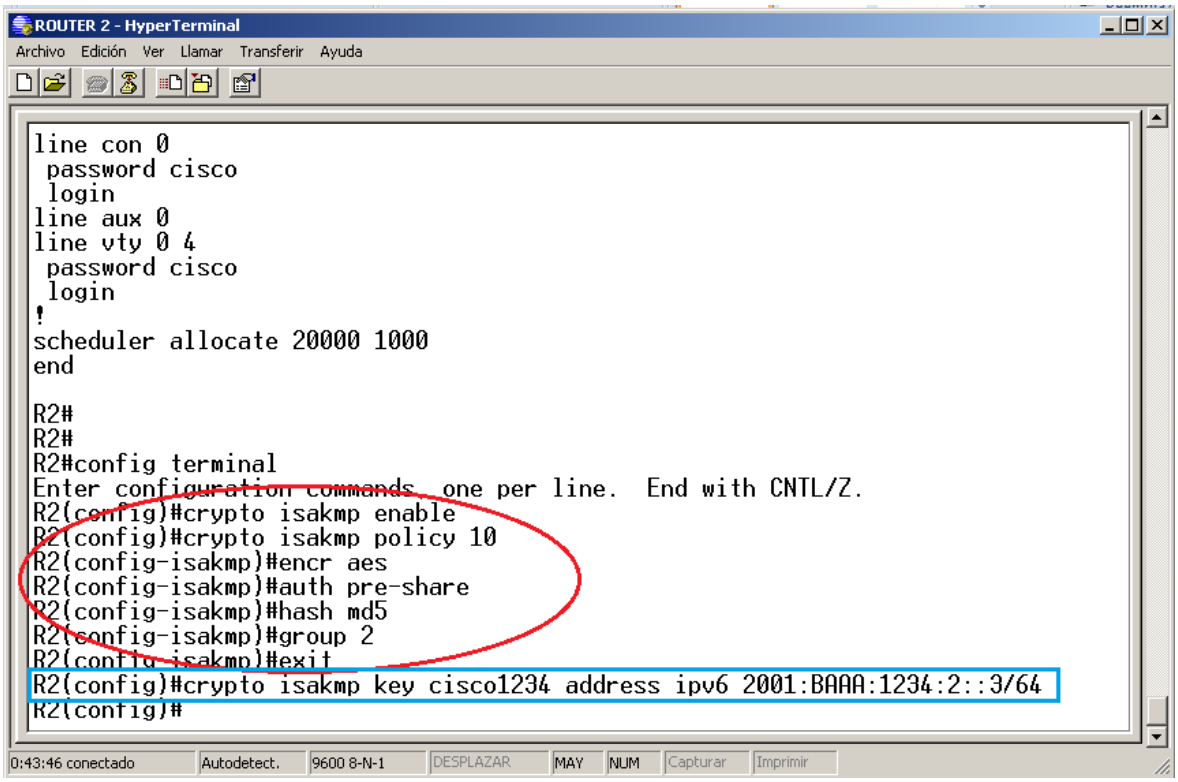


FIG.4.4-65 Implementación de la Política IKE en Fase I (Router 1, 2)

Fuente: Resultado de la Investigación

4.4.6.2 FASE II

La Fase II del protocolo IKE se define las seguridades a través de la IPSec, que ofrece dos modos de operación como Modo de transporte o Modo Túnel. En el siguiente punto se detalla la sintaxis de la implementación.

De acuerdo a los comandos que se implemento en la Fase 1 (MD5, PRE-SHARE, AES) se debe relacionar los mismos comandos en la Fase 2 para la política de IPsec de acuerdo a lo elegido

FASE 2

POLITICA IPSEC
ah-md5-hmac
ah-sha-hmac
esp-des
esp-md5-hmac
esp-sha-hmac
esp-null

Tabla 4.4-16 Fase 2 del protocolo IKE

Fuente: Resultados de la Investigación

4.4.6.2.1 IMPLEMENTACION DEL PROTOCOLO IPSEC

ROUTER 1

1._ Paso

Se debe configurar IPsec en cada extremo, se configura el transform-set es el que define las políticas de seguridad que serán aplicadas al tráfico que entra o sale de la interfaz, para lo cual utiliza el siguiente comando:

crypto ipsec transform-set transform-set-name (transform 1) (transform 2)

crypto ipsec transform-set myset esp-aes esp-md5-hmac

//Configuración de la transformada ESP que es un mecanismo para el cifrado del payload, se elije un protocolo de encriptación ESP, el algoritmo AES, y el algoritmo MD5, porque son los que se eligió en la Fase 1 //

Se usa modo túnel para que todos los paquetes IP estén cifrados/autentificados, también para que la comunicación sea de red a red (túneles seguros entre routers VPNs) o de una host a una red. En cambio el modo transporte se usa solo para una comunicación de un Host a Host.

mode tunnel //Habilita modo tunnel//

exit //Vuelve al modo de configuración global//

2._ Paso

crypto ipsec profile myprofile1

//Definen los parámetros de IPSec que serán usados por la encriptación de IPsec entre 2 routers IPsec //

set-transform-set myset //Activa IPSec SA para que el tráfico pueda pasar, y tiene que ser el mismo nombre que se creó en crypto ipsec transform-set, para que se pueda activar //

exit //Vuelve al modo de configuración global//

ROUTER 2

1._ Paso

Se debe configurar IPsec en cada extremo, se configura el transform-set es el que define las políticas de seguridad que serán aplicadas al tráfico que entra o sale de la interfaz, para lo cual utiliza el siguiente comando:

crypto ipsec transform-set transform-set-name (transform 1) (transform 2)

crypto ipsec transform-set myset esp-aes esp-md5-hmac

//Configuración de la transformada ESP que es un mecanismo para el cifrado del payload, se elije un protocolo de encriptación ESP, el algoritmo AES, y el algoritmo MD5, porque son los que se eligió en la Fase 1 //

Se usa modo túnel para que todos los paquetes IP estén cifrados/autentificados, también para que la comunicación sea de red a red (túneles seguros entre routers VPNs) o de una host a una red. En cambio el modo transporte se usa solo para una comunicación de un Host a Host.

mode tunnel //Habilita modo túnel//

exit //Vuelve al modo de configuración global//

2._ Paso

crypto ipsec profile myprofile1

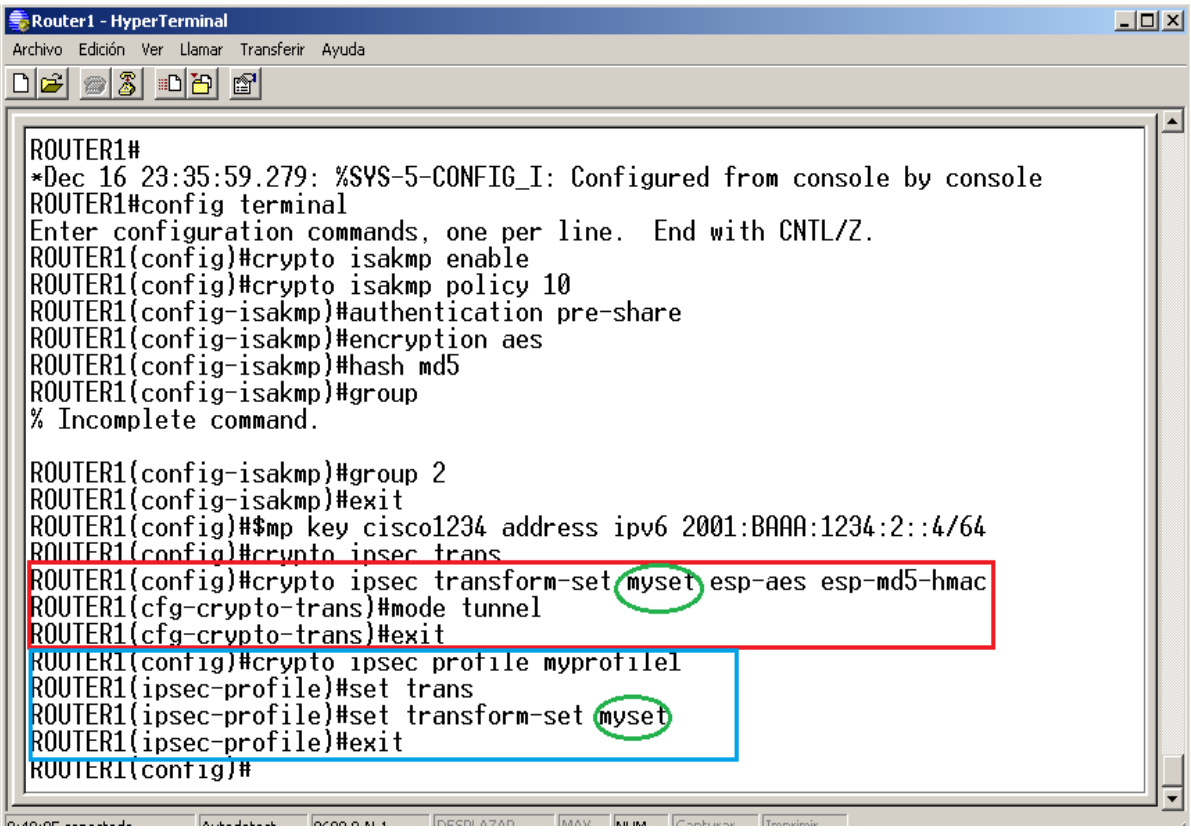
//Definen los parámetros de IPSec que serán usados por la encriptación de IPsec entre 2 routers IPsec //

set-transform-set myset //Activa IPSec SA para que el tráfico pueda pasar, y tiene que ser el mismo nombre que se creó en crypto ipsec transform-set, para que se pueda activar //

exit //Vuelve al modo de configuración global//

En esta Fase tanto en el Router 1 como el Router 2 deben ser configurados de forma igual para que la conexión entre los routers funcione.

Se debe tener en cuenta que el nombre del transform-set debe ser el mismo nombre dentro del comando ipsec profile.



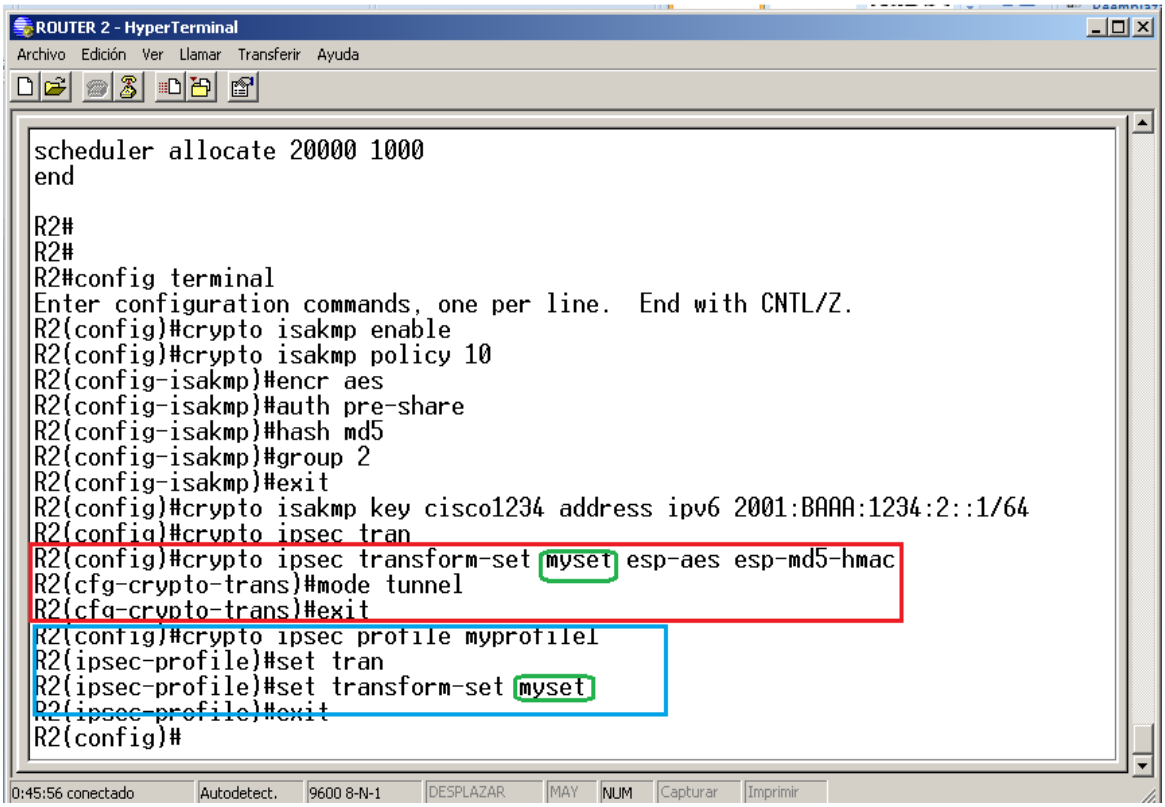


FIG.4.4-66 Implementación de la Política IKE en Fase II (Router 1, 2)

Fuente: Resultado de la Investigación

4.4.7 IMPLEMENTACION DE LISTAS DE ACCESO

Las ACLs permiten controlar el flujo del tráfico en equipos de redes. Su principal objetivo es filtrar tráfico, y para aplicar una política de seguridad que permite o niega el acceso de cierta parte de la red a otra. La granularidad de las ACLs permite que estas partes sean o bien un Host específicos o partes de una subred arbitrariamente, es decir, permiten que se conceda o niegue el acceso desde un único Host hasta otro, de un segmento de red a otro o cualquier combinación que se quiera

Se usa Acceso de Lista en esta topología porque se necesita filtrar el tráfico que entra o sale de la red de esta manera la información podrá viajar por el túnel y se

conocerá cuantos paquetes serán encriptados, encapsulados. Si no se crea listas de accesos el tráfico y la información no pasa por el túnel.

Sintaxis:

ipv6 access-list <name> : Son usados para filtrar el tráfico y restringir el acceso para el router.

[no] permit | deny ipv6 | <protocol> any | host <src> | src/len [sport] any | host <dest> | dest/len [dport] [reflect <name> [timeout <secs>]] [fragments] [routing] [dscp <val>] [flow-label <val>][time-range <name>] [log | loginput] [sequence <num>]

ROUTER 1

1._ Lista de Acceso Extendida

Ipv6 access-list acl_in //Crea una lista de acceso cuando el tráfico entre//

permit ipv6 2001:AAAA:1234:1::2/64 2001:AAAA:1234:2 ::2/64

//Permite el acceso desde el Host A al Host B//

permit ipv6 any any //Permite el acceso si las condiciones están dentro del rango//

exit //Vuelve al modo de configuración global//

2._ Lista de Acceso Extendida

Ipv6 access-list acl_out //Crea una lista de acceso cuando el tráfico salga //

permit udp host 2001:BAAA:1234:2::4 host 2001:BAAA:1234:2::3 eq 500

//permite el acceso a través del protocolo UDP con el puerto 500//

permit esp host 2001:BAAA:1234:2::4 host 2001:BAAA:1234:2::3

//permite el acceso a través ESP//

permit ipv6 2001:AAAA:1234:2::2/64 2001:AAAA:1234:1 ::2/64

//permite el acceso desde el Host B al Host A//

permit ipv6 any any //Permite el acceso si las condiciones están dentro del rango//

exit //Vuelve al modo de configuración global//

ROUTER 2

1._ Lista de Acceso Extendida

lpv6 access-list acl_in //Crea una lista de acceso cuando el tráfico entre//

permit ipv6 2001:AAAA:1234:2::2/64 2001:AAAA:1234:1 ::2/64

//permite el acceso desde el Host B al Host A//

permit ipv6 any any //Permite el acceso si las condiciones están dentro del rango//

exit //Vuelve al modo de configuración global//

2._ Lista de Acceso Extendida

lpv6 access-list acl_out //Crea una lista de acceso cuando el tráfico salga //

permit udp host 2001:BAAA:1234:2::3 host 2001:BAAA:1234:2::4 eq 500

//permite el acceso a través del protocolo UDP con el puerto 500//

permit esp host 2001:BAAA:1234:2::3 host 2001:BAAA:1234:2::4

//permite el acceso a través ESP//

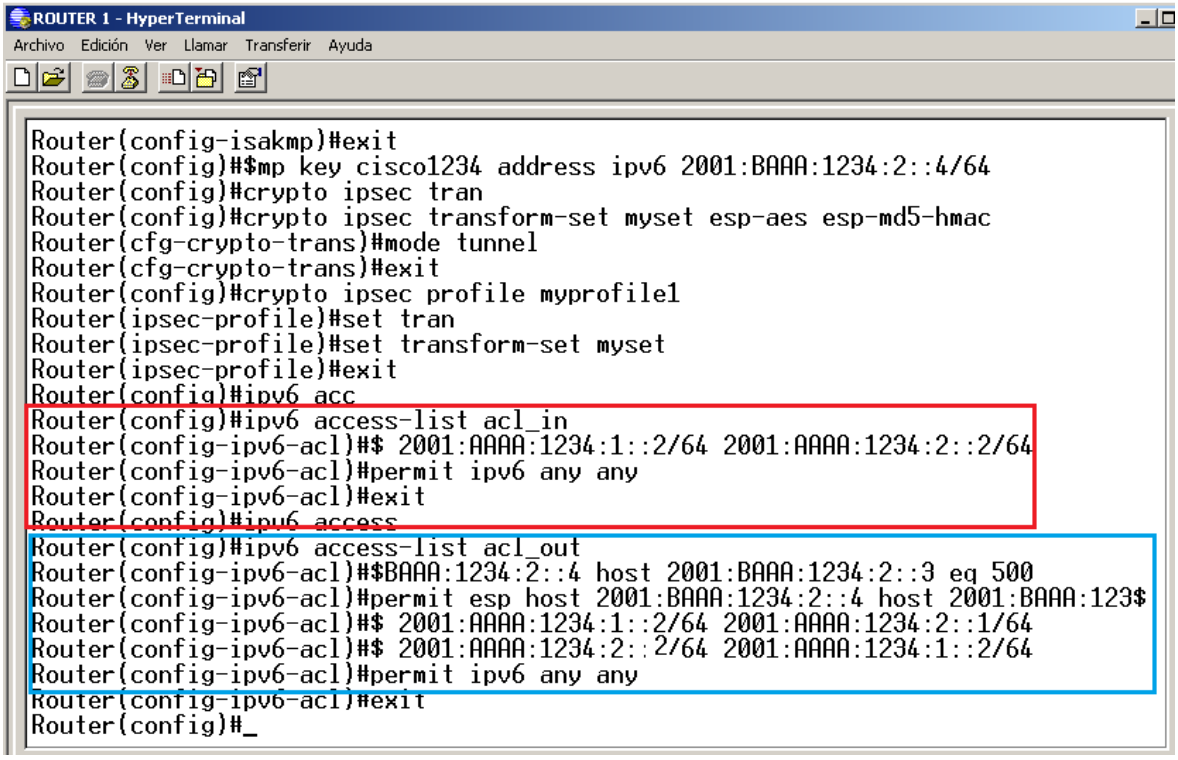
permit ipv6 2001:AAAA:1234:1::2/64 2001:AAAA:1234:2 ::2/64

//permite el acceso desde el Host A al Host B//

permit ipv6 any any //Permite el acceso si las condiciones están dentro del rango//

exit //Vuelve al modo de configuración global//

Para que las listas de acceso funcionen se debe activar en cualquier interfaz de los routers.



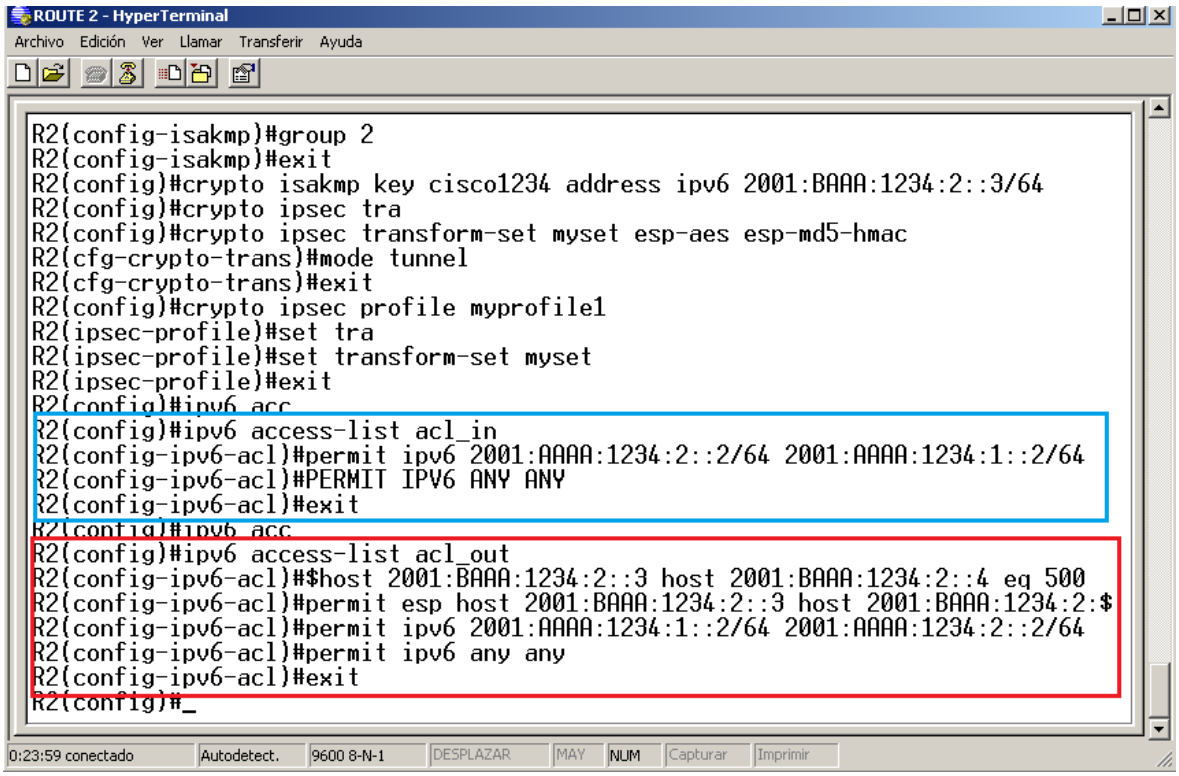


FIG.4.4-67 Implementación de Listas de Acceso (Router 1, 2)

Fuente: Resultado de la Investigación

4.4.8 IMPLEMENTACION DEL TUNEL PARA EL TRÁFICO IPv6

La creación del Túnel permitirá que el tráfico que circule por la red pase por el túnel para que las listas de acceso se puedan activar en esta interfaz y cuando la información llegue a su destino estará encriptada.

Sintaxis

Router 1

```
Ipv6 cef                          //Crea una lista de acceso cuando el tráfico entre//
Interface tunnel 0                /Se crea un Túnel 0//
Ipv6 address 2001:ABAA:1234:1::1/64
//Proporciona una dirección Ipv6 para este túnel, para que el tráfico Ipv6 pueda tener una ruta//
Ipv6 enable                       // activa el protocolo IPv6//
Ipv6 cef
tunnel source 2001:BAAA:1234:2::3          // Pone una dirección de origen en el Túnel//
tunnel destination 2001:BAAA:1234:2::4     // Especifica el destino para el Túnel//
tunnel mode ipsec ipv6                     // Coloca un medio de la encapsulación en el túnel//
tunnel protection ipsec profile myprofile1 // Asocia la interfaz del túnel con IPsec Profile //
ipv6 traffic-filter acl_in in              // Activa la lista de acceso//
ipv6 traffic-filter acl_out out            // Activa la listas de acceso//
exit                                       //Vuelve al modo de configuración global//
```

Router 2

```
Ipv6 cef                          //Crea una lista de acceso cuando el tráfico entre//
Interface tunnel 0                //Crea un Túnel 0//
```

Ipv6 address 2001:ABAA:1234:1::2/64

//Proporciona una dirección Ipv6 para este túnel, para que el tráfico Ipv6 pueda tener una ruta//

Ipv6 enable // activa el protocolo IPv6//

Ipv6 cef

tunnel source 2001:BAAA:1234:2::4 // Pone una dirección de origen en el Túnel//

tunnel destination 2001:BAAA:1234:2::3 // Especifica el destino para el Túnel//

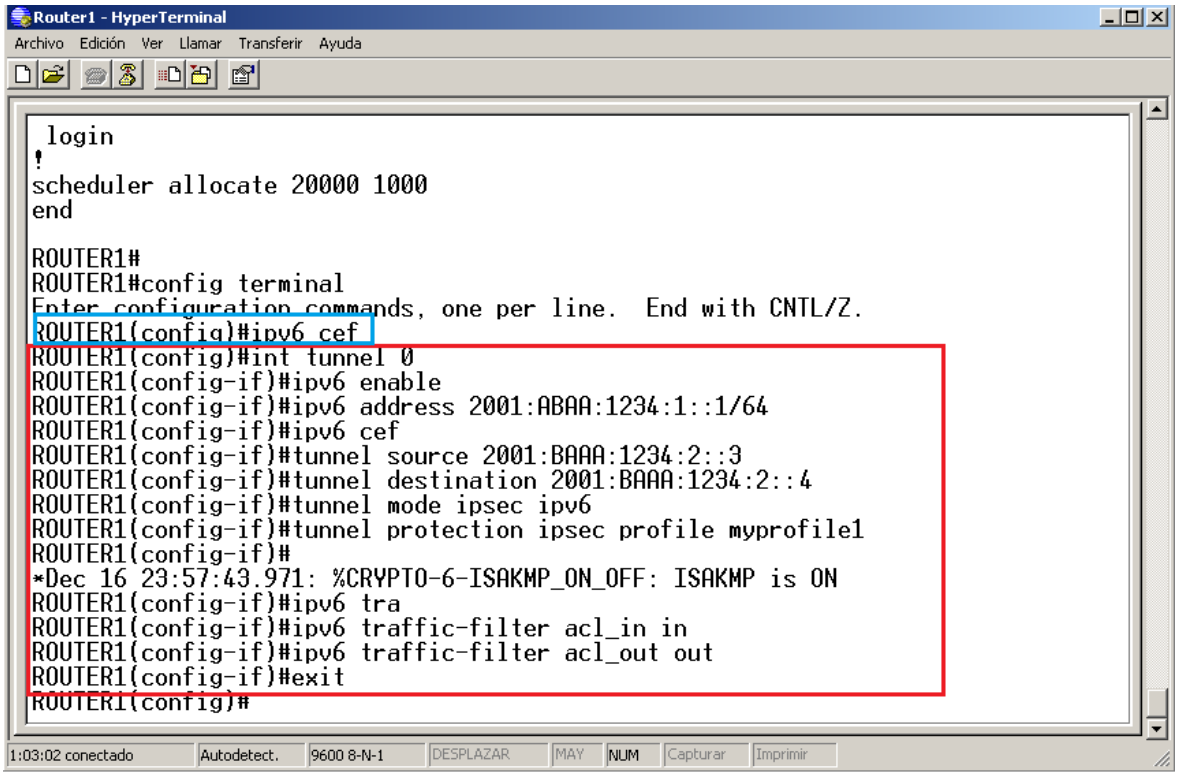
tunnel mode ipsec ipv6 // Coloca un medio de la encapsulación en el túnel//

tunnel protection ipsec profile myprofile1 // Asocia la interfaz del túnel con IPsec Profile //

ipv6 traffic-filter acl_in in // Activa la lista de acceso//

ipv6 traffic-filter acl_out out // Activa la lista de acceso//

exit //Vuelve al modo de configuración global//



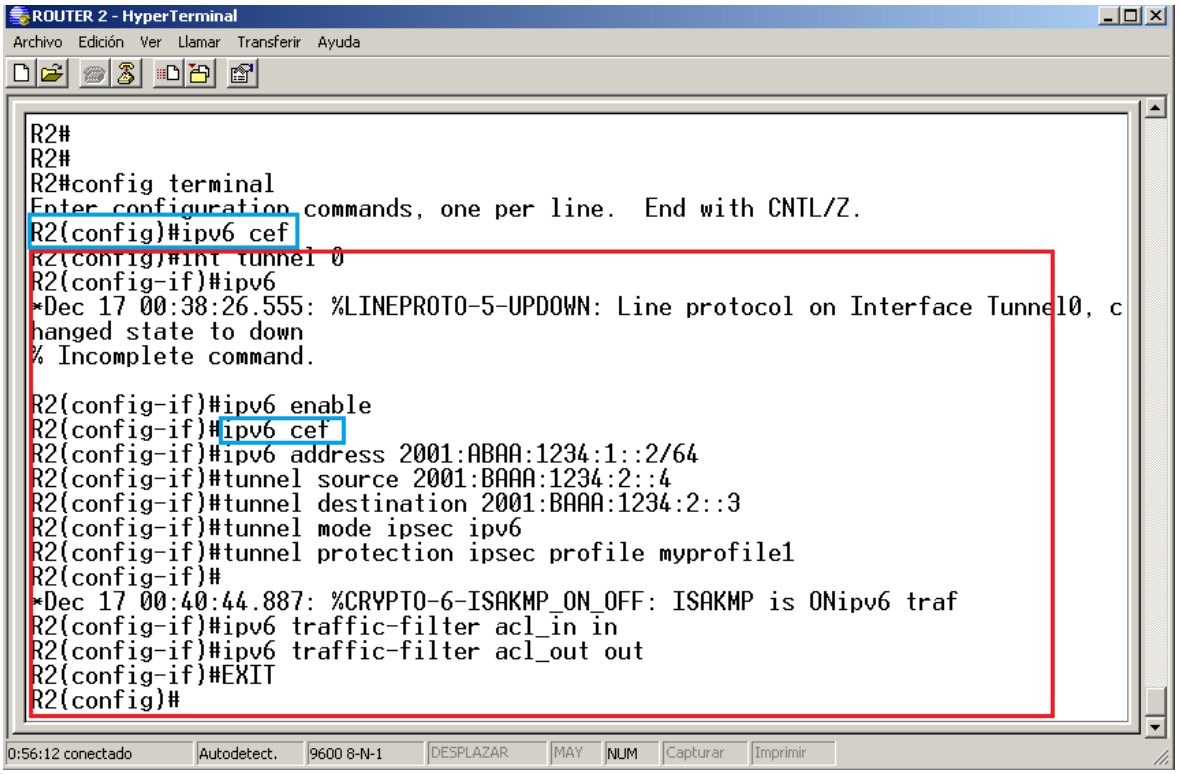


FIG.4.4-68 Implementación del Túnel (Router 1, 2)

Fuente: Resultado de la Investigación

4.5 VERIFICACION DE CONECTIVIDAD ENTRE LOS HOST A y B

La conectividad entre el Host A al Host B se puede verificar haciendo un ping6 desde el Host A al Host B y viceversa.

Para conocer cuántos paquetes están encriptado desde un host al otro se verifica en el router con show crypto ipsec sa

1._ Ping6 del Host A al Host B

Para conocer la funcionalidad de cada protocolo de seguridad en IPv6, primero se debe hacer un ping desde el Host A al Host B o viceversa, de esta manera se verifica la conectividad, es importante realizar el ping porque los paquetes que se envíen desde el Emisor al Receptor serán encriptados siempre y cuando los protocolos IPsec, ISAKMP, IKE estén activados

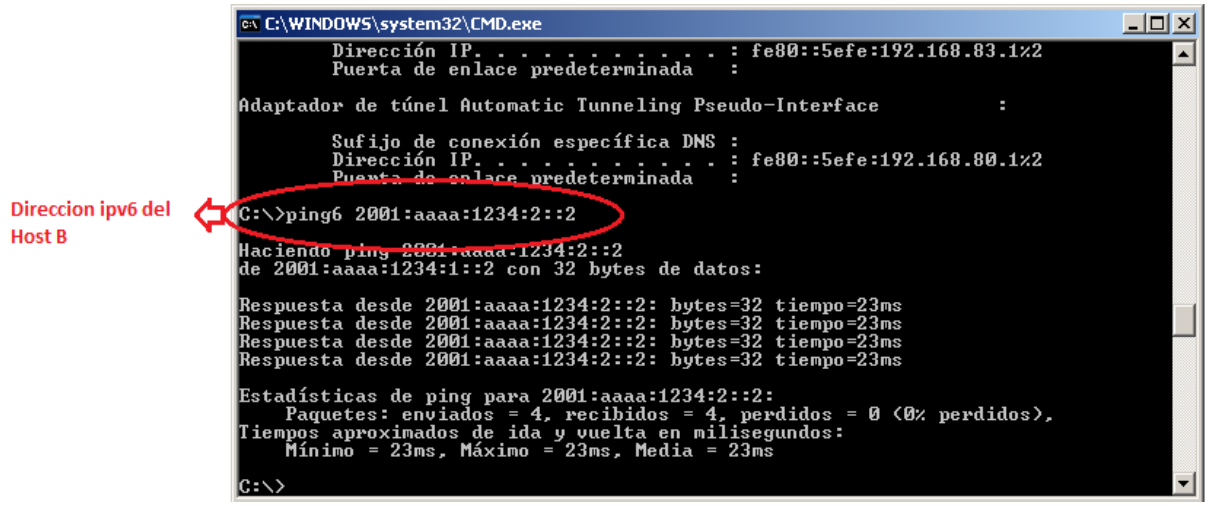


FIG.4.4-69 Verificación de Conectividad entre Hosts

Fuente: Resultado de la Investigación

2._ Show crypto ipsec sa

Una vez realizado el ping para verificar la conectividad, se puede comprobar los protocolos de seguridad mediante el comando show crypto ipsec sa, que están activados como se muestra en la figura 4.4-70. Para verificar los protocolos de Seguridad los paquetes deben pasar por el túnel donde se activa las ACLs como el protocolo IPSec, ISAKMP en caso de no activar, los paquetes no llegarán encriptados ni encapsulados y al hacer ping de un host a otro solo se comprueba la conectividad pero los paquetes no pasan por el túnel y los protocolos de seguridad no estarán en funcionamiento en la red.

Si en el comando crypto ipsec profile no se activa ipsec transform-set, el tráfico no pasara por el túnel y el protocolo IPSec no funcionará, los paquetes no se verán cuantos llegaron encapsulados y cuando se realice el comando show crypto ipsec sa se desplegara que no se encuentra la SA

En los Anexo E se encuentran los gráficos de la conectividad de ISAKMP e IPSec de acuerdo a las fases IKE que se detalló en los puntos anteriores de este capitulo

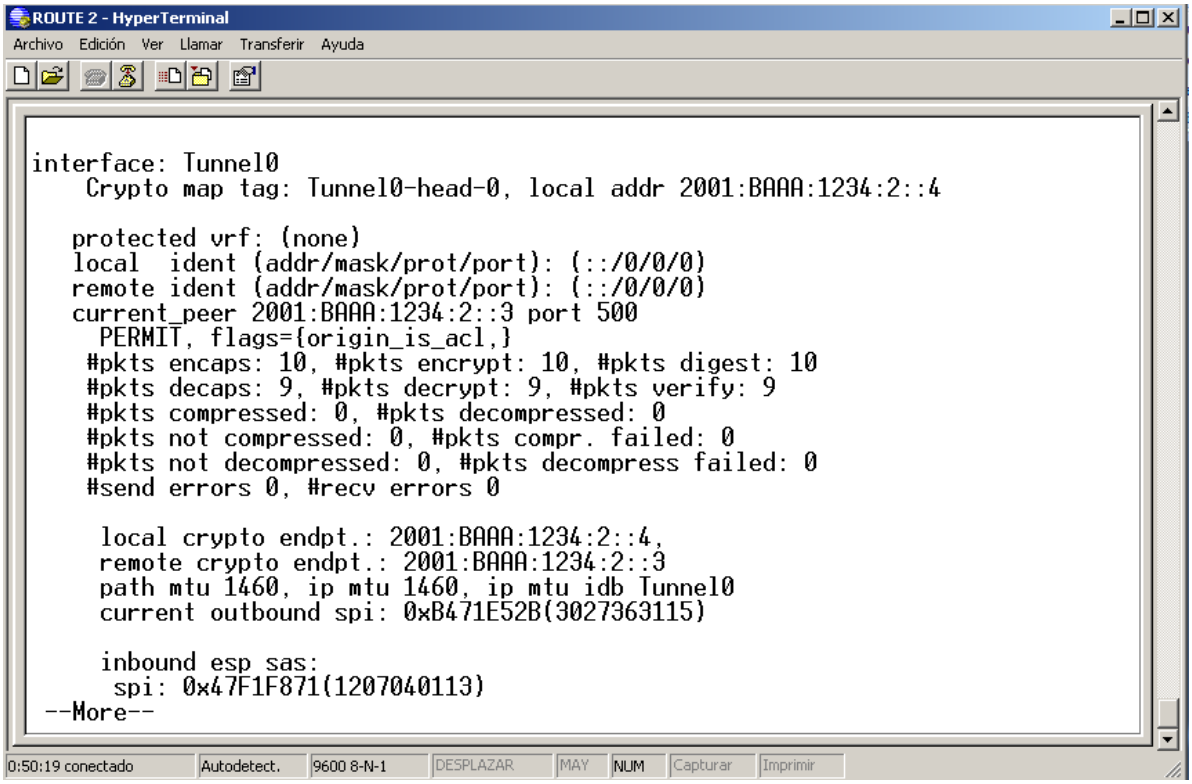


FIG.4.4-70 Verificación de paquetes Encriptados

Fuente: Resultado de la Investigación

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- El propósito de este proyecto es poder analizar las funcionalidades de los protocolos de seguridad IPSec, IKE e ISAKMP sobre IPv6 permitiendo demostrar la seguridad de la información como la funcionalidad y ventajas que presentan estos protocolos bajo la infraestructura Cisco con equipos 2801.

- El crecimiento de usuarios en las redes actuales permitirá el cambio de IPv4 a IPv6 no como un remplazo, sino como un sucesor de integraciones y evoluciones potentes y flexibles, ofreciendo servicios de seguridad como la confidencialidad de la información como la autentificación e integridad.

- IPsec proporciona servicios de seguridad en Internet y es una buena solución para los requerimientos de encriptación, autentificación, permitiendo a un sistema seleccionar los protocolos de seguridad, determinar los algoritmos a utilizar para los servicios, e implementar cualquier algoritmo criptográfico requerido para proporcionar los servicios solicitados y logrando que estos sean transparentes al usuario final.

- Con la investigación realizada para los diferentes protocolos de seguridad que se implementó, se determina la interconexión de dos redes diferentes por medio de rutas estáticas, las mismas que establecen la comunicación de un extremo a otro extremo utilizando listas de acceso para aplicar una política de seguridad que permite o niega el acceso de cierta parte de la red a otra y cuando la información viaje por el túnel, logre que esté encriptada y cuando llegue al receptor será el único que pueda descifrarlo.

- De acuerdo a la investigación se determino el estudio de las rutas estáticas por la topología elegida como es punto a punto y una de las características de las rutas estáticas es la seguridad y el ahorro de recursos del router y

no había la necesidad de generar rutas dinámicas, que son actos para una topología de mas nodos.

- De acuerdo a las políticas del Protocolo IKE se debe realizar una combinación de fases de seguridad que serán usadas durante la negociación con los protocolos ISAKMP, IPSec, estos permiten el uso de una infraestructura de red pública para establecer una comunicación privada, es decir proporciona un mecanismo para la construcción de redes privadas virtuales.

- Se debe tener en cuenta que el túnel creado es para que el tráfico pueda ser activado o la información pueda viajar dentro de este y las diferentes listas de acceso se activen, y no para convertir una dirección IPv4 en IPv6 dentro del túnel.

5.1 RECOMENDACINES

- Cuando se realice una práctica de los protocolo de seguridad IPSec, ISAKMP, IPsec se recomienda que las listas de acceso sean extendidas y se creen dos tipos de lista una cuando el tráfico entra y otra cuando salga, de esta manera el tráfico podrá pasar por el túnel y será activado.

- Se recomienda que los nombres que piden en las diferentes criptografías como por ejemplo ipsec transform-set **myset** sea el mismo nombre (myset) donde se vuelva a llamar en otros comandos porque si no llevan el mismo nombre IPsec SA no se activara y los paquetes no se pueden encriptar. En los gráficos del capítulo IV están marcados los nombres que deben ser iguales.

- Se recomienda continuar con el estudio y/o investigación del protocolo IPv6 para poder implementar en diferentes aéreas la funcionalidad de IPv6, como su calidad de servicio (QoS) o poder implementar IPv6 en Oracol Solaris.

BIBLIOGRAFIA

REFERENCIAS BIBLIOGRAFICAS

- Ghislayne Xiomara Vera: Diseño de la Transición de direcciones IPv4 a IPv6:2009: Zamora.

- Gabriel Verdejo Álvarez: El protocolo IPv6 y sus extensiones de seguridad IPSec: Universidad Autónoma de Barcelona: Febrero 2000: Bellaterra.

- Hugo Adrian Francisconi: IPSec en Ambiente IPv4 e IPv6: Primera Edición (Volumen I): Agosto 2005: Argentina.

- Raúl Borras Gonzales: Proyecto de Interconexión: Universidad Politécnica Cataluña: Febrero 2007.

- Edison Rafael Trujillo Machado: Diseño e Implementación de una VPN en una Empresa Comercializadora Utilizando IPSec: Universidad Politécnica Nacional: Marzo 2006: Quito.

- Jorge Enrique López Logacho: “Diseño de una red prototipo bajo IPv6 basado en los protocolos de enrutamiento RIP Y OSP”: Universidad Politécnica Salesiana: Julio 2007 Quito.

- Neal Ziring: Router Security Configuration Guide Supplement-Security for IPv6 Routers: Mayo 2006: United States of American

- Víctor Villagra: Universidad de México; @2000, DIT-UPM

- Peralta, Luis. IPv6 @ UJI - Rev : 22, , Febrero de 2002

- Rivest, R., "The MD5 Message Digest Algorithm", RFC 1321, April 1992

- Knowledgenet.Cisco.Securing.Networks.with.PIX.and.ASA.SNPA.Student. Guide.V4.0.eBook-DDU.pdf

REFERENCIAS DE INTERNET

- http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/ip.htm
- http://www.linuxchile.cl/docs.php?op=imprimirVersion&doc=16&id=1l
- http://www.monografias.com/trabajos30/direccionamientoip/direccionamiento-_ip.shtml
- http://es.wikipedia.org/wiki/Direcci%C3%B3n_IP
- http://www.ipv6.codarec.frm.utn.edu.ar/
- http://www.linuxchile.cl/docs.php?op=imprimirVersion&doc=16&id=1l
- http://www.freebsd.org/doc/es/books/handbook/network-ipv6.html
- http://fmc.axarnet.es/tcp_ip/tema-03/tema-03.htm
- http://antonio_gallego.tripod.com/apuntes/listas.htm
- http://es.wikipedia.org/wiki/Internet
- http://www.nodo50.org/manuales/internet/1.htm#superior
- http://www.economicas-online.com/interser.htm
- http://www.saulo.net/pub/tcpip/a.htm
- http://www.mailxmail.com/curso-que-son-redes/que-es-tcp-ip
- http://es.wikipedia.org/wiki/Modelo_OSI
- http://www.textoscientificos.com/redes/tcp-ip/capas-arquitectura-tcp-ip
- http://es.wikipedia.org/wiki/Transmission_Control_Protocol
- http://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/tcp.html
- http://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/conextcp.html
- http://neo.lcc.uma.es/evirtual/cdd/tutorial/transporte/udp.html

- http://technet.microsoft.com/es-es/library/cc785220(WS.10).aspx
- http://es.wikipedia.org/wiki/User_Datagram_Protocol
- http://www.freebsd.org/doc/es/books/handbook/network-ipv6.html
- http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf
- http://www.rediris.es/red/iris-ipv6/direccionamientoipv6.html
- http://www.cryptography.com
- http://www.cs.hut.fi/crypto
- http://www.cs.hut.fi/ssh/crypto/algorithms.html

ANEXOS A

GLOSARIO

Algoritmo: conjunto de reglas bien definidas para la resolución de un problema. Un programa de software es la transcripción, en lenguaje de programación, de un algoritmo.

ARP (Protocolo de Resolución de Direcciones): Un protocolo de resolución de direcciones electrónicas en números IP que corre en redes locales. Parte del conjunto de protocolos TCP/IP.

ARPANET (Red de la Agencia de Proyectos de Investigación Avanzados): Una red pionera de computadoras, fundada por DARPA, una agencia de investigación del gobierno norteamericano. Fue la base fundamental en los años sesenta para el desarrollo de lo que luego se convertiría en la red Internet.

Bit: El bit es la unidad más pequeña de almacenamiento en un sistema binario dentro de una computadora.

Cabecera: (Header): Información que suele situarse delante de los datos (por ejemplo en una transmisión) y que hace referencia a diferentes aspectos de estos.

Capa (Layer): Cada una de los elementos que conforman una estructura jerárquica.

Comercio electrónico (E-comerce): Actividad que consiste en la compra o venta de artículos por IInternet.

DARPA: Defense Advanced Research Projects Agency.

Datagrama: Conjunto de estructurado de bytes que forma la unidad básica de comunicación del protocolo IP (en todas sus versiones).

Dirección Anycast: Un identificador para un conjunto de interfaces (típicamente pertenecientes a distintos nodos). Un paquete enviado a una dirección multicast se entrega a uno de los interfaces identificado por esa dirección (el "más cercano", según la medida de distancia del protocolo.

Dirección Multicast: Es un identificador para un grupo de interfaces, ejemplo un paquete es enviado a una dirección multicast y es entregado a todas aquellas interfaces identificadas por esa dirección.

Encaminamiento (Routing): Procedimiento que consiste en conducir un datagrama hacia su destino a través de Internet.

Encapsulamiento: Sistema basado en colocar una estructura dentro de otra formando capas.

Encriptación: Método de seguridad por el cual los datos son convertidos en otros por medio de procedimientos de seguridad, con el fin de que la información no sea leída por nadie.

Ethernet: El método más usado de acceso a una LAN (Estándar IEE 802.3)

FTP: File Transfer Protocol (Protocolo de Transferencia de Ficheros).

Host: Es un nodo que no es un enrutador. Computador, Anfitrión.

IANA.: Son las siglas en inglés de la “Internet Assigned Numbers Authority”.

ICANN: Son las siglas en inglés de la “Internet Corporation of Assigned Numbers and Names”.

ICMP (Internet Control Message Protocol): Protocolo encargado de la comunicación de mensajes entre nodos conectados a Internet.

I**CV**: Valor de Comprobación de Integridad (Integrity Check Value)

IKE: Intercambio de Claves en Internet (Internet Key Exchange)

Interface: Lo que acopla un nodo a un enlace.

Internet: Red de redes a escala mundial de millones de computadoras interconectadas con el conjunto de protocolos TCP/IP.

IP (Internet Protocolo): Protocolo no fiable y sin conexión en el que se basa la comunicación por Internet. Su unidad es el datagrama.

IPsec: Seguridad IP (IP Security)

I**Pv4:** IP version 4 (IP Version 4)

IPv6 (IP versión 6): Abreviatura escogida en IETF [WWW 16] con la que se denomina la versión 6 del protocolo IP.

ISAKMP: Protocolo de Manejo de Claves y Asociaciones de Seguridad en Internet (Internet security association and key management protocol)

LAN (Local Area Network): Red local. Es la encargada de conectar computadoras en distancias inferiores a 1Km.

MAC Address: Dirección única que llevan las tarjetas de red grabadas en una ROM para identificarse y diferenciarse de las demás.

MTU (Maximun Transfer Unit): Siglas que denominan el tamaño máximo en unidades de transmisión que se permite en un canal de comunicación.

OSI (Modelo): Modelo teórico propuesto por IEEE que describe cómo deberían conectarse distintos modelos de computadoras a diferentes tipos de red para poder comunicarse entre sí.

Overhead: Pérdida de rendimiento.

Paquetes: Ver datagrama.

Protocolos: Conjunto de reglas que establece cómo debe realizarse una comunicación.

Red: Dispositivo físico que conecta dos o más computadoras.

RFC (Request For Comments): Documento de especificaciones que se expone públicamente para su discusión.

Router: Dispositivo físico u ordenador que conecta dos o más redes encargado de direccionar los distintos datagramas que le lleguen hacia su destino.

SPD: Base de Datos de Políticas de Seguridad (Security Policy Database).

SPI: Índice de Parámetros de Seguridad (Security Parameters Index).

SSL (Secure Socket Layer): Protocolo que proporciona seguridad en Internet a partir del protocolo TCP.

TCP (Transmission Control Protocol): Protocolo de nivel superior que permite una conexión fiable y orientada a conexión mediante el protocolo IP.

UDP (User Datagram Protocol): Protocolo no fiable y sin conexión basado en el protocolo IP.
VPN: Red privada virtual (Virtual private network).

WAN: Red de gran alcance. Este tipo de red suele utilizarse en la unión de redes locales (LAN).

ANEXO B

RFC

	Documento	Título
Especificaciones Básicas	RFC2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
	RFC2462	Autoconfiguración de Direcciones "stateless" IPv6
	RFC2463	Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)
	RFC1981	Descubrimiento del MTU de la ruta para IPv6
	RFC1809	Uso del campo "Etiqueta de Flujo" en IPv6
Direccionamiento	RFC2373	Arquitectura de Direccionamiento en IPv6
	RFC1887	Arquitectura para la Asignación de Direcciones Unicast IPv6
	RFC2374	Formato de Direcciones Unicast Agregables Globales
IPv6 sobre ...	RFC2464	Transmisión de paquetes IPv6 sobre redes Ethernet
	RFC2472	IPv6 sobre PPP
	RFC2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast
	RFC2492	IPv6 sobre redes ATM
Seguridad	RFC2401	Arquitectura de Seguridad para IP
	RFC2402	Cabecera de Autenticación IP
	RFC2406	Encriptación de datos en IP (ESP)

	RFC2408	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)
Multicast	RFC2375	Asignación de Direcciones Multicast
	RFC2710	Descubrimiento de nodos que desean recibir Multicast para IPv6
Anycast	RFC2526	Direcciones de Subredes para Anycast en IPv6
Transición	RFC1933	Mecanismos de Transición para Routers y Hosts IPv6
	RFC2185	Aspectos de Routing de la Transición IPv6
	RFC2473	Especificaciones Genéricas de Tunelización de Paquetes en IPv6
	RFC2529	Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos
Otros	RFC1881	Gestión de la Asignación de Direcciones IPv6
	RFC1924	Representación Compacta de Direcciones IPv6
	RFC2147	TCP y UDP sobre IPv6
	RFC2428	Extensiones FTP para IPv6 y NAT
	RFC2471	Plan de Asignación de direcciones IPv6 para Pruebas

ANEXO C

ACTUALIZACION DE LAS IOS DEL ROUTER

En este documento se describe como copiar, restaurar y borrar la configuración de un dispositivo Cisco. Previo al procedimiento de copia se debe disponer de la contraseña para poder entrar en el modo de ejecución privilegiado, en caso del router contenga passsword.

Para actualizar la IOS de un router Cisco, se necesita un programa Cliente TFTP como el Cisco TFTP Server instalado en el computador. Una vez hecho esto, abrir en el computador el programa Cisco TFTP Server; se lo configura para que en la opción TFTP Server root Directory= (Directorio donde está el archivo Flash), sea la fuente del archivo .bin que será la fuente de actualización .
Una vez configurado el programa Cisco TFTP Server, acceder al router mediante telnet o hyperterminal.

Copia de la IOS del Route al PC

Una vez arrancado y configurado el servidor TFTP, ejecutar el comando copy flash: tftp: en modo de ejecución privilegiado, cuando se ejecute, pedirá el nombre del fichero que está en la flash, luego la IP o nombre del servidor TFTP, finalmente pedirá el nombre del fichero a grabar en el servidor TFTP.

Router> enable
Router# copy flash tftp
Source Filename []? (nombre del archivo IOS)
Address or name of remote host []? (IP del Router)
Destination Filename []? (nombre del archivo IOS)
!!!
!!!
!!!
!!!
!!!
!!!
!!!
!!!

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
3802992 bytes copied in 27.276 secs (140851 bytes/sec)
```

Cargar la IOS del PC al Router

El proceso para restaurarla, es igual que el anterior caso, pero ahora el origen no será la flash, sino el servidor TFTP y el destino será la flash, por lo tanto el comando a ejecutar en el modo privilegiado será copy tftp: flash:

Cuando este comando sea ejecutado lo primero que pedirá será la IP o nombre del servidor TFTP, seguidamente preguntará que archivo se quiere copiar del TFTP, y luego preguntará con que nombre se desea grabar el archivo. En el caso que este archivo se encuentre en la flash pedirá si se quiere sobrescribirlo y luego preguntará si se desea borrar toda la flash. En el caso que se conteste afirmativamente, lo volverá a preguntar para asegurarse, ya que se perderá todo el contenido de la flash. Para finalizar, borrará la flash y grabará el nuevo fichero.

```
Router# copy tftp flash
Address or name of remote host []? (IP del computador que tiene el TFTP)
Source Filename []? (nombre del archivo IOS)
Destination Filename []? (nombre del archivo IOS)
Warning:There is a file already existing with this name
Do you want to over write? [confirm]
Accessing tftp://xxx.xxx.xxx.xxx/c827v-y6-mz.121-1.XB...
Erase flash: before copying? [confirm]
Erasing the flash filesystem will remove all files! Continue? [confirm]
Erasing device...
eeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeeee
ee ...erased
Erase of flash: complete
Loading c827v-y6-mz.121-1.XB from 10.1.1.1 (via Ethernet0): !!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
[OK - 3802992/7605248 bytes]
Verifying checksum... OK (0x1ABC)
3802992 bytes copied in 58.236 secs (65568 bytes/sec)
```

Una vez reiniciado el Router, comprobar la versión instalada con el siguiente comando:
Router> show versión
Comprobar si la versión del router se ha actualizado.

Borrar la configuración de un dispositivo Cisco

Para borrar la configuración de un dispositivo Cisco, se debe, antes de nada, entrar en el modo de ejecución privilegiado (comando enable desde el modo de ejecución de usuario), después ejecutar el comando erase startup-config, una vez ejecutado, confirmará si la NVRAM del sistema se ha borrado. Una vez realizado esto, se debe apagar y encender de nuevo el router (o ejecutar el comando reload en el modo de ejecución privilegiado) y quedará completamente borrado. Cuando se inicie, preguntará si se quiere acceder a un asistente para establecer una configuración inicial del router.

```
Router#erase startup-config
Erasing the nvram filesystem will remove all files! Continue?
[confirm]
[OK]
Erase of nvram: complete
```

Al realizar el reset al router y cargado el IOS, saldrá esta pregunta:

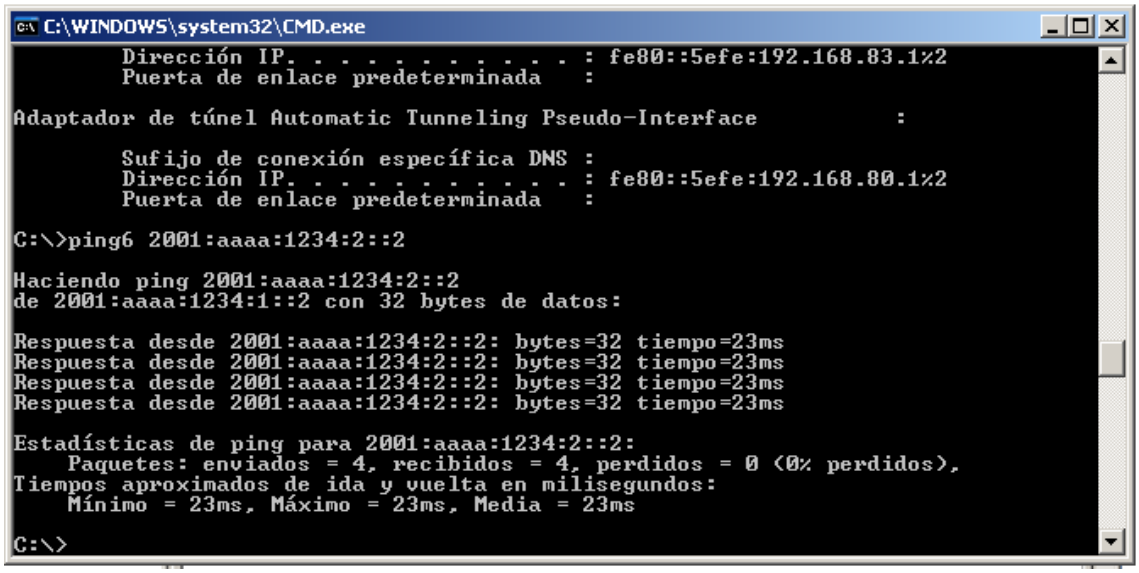
```
--- System Configuration Dialog ---
Would you like to enter the initial configuration dialog? [yes/no]: no
```

Si se ejecutan los comandos enable y show running-config, se observa que la configuración está vacía.
Si por error se ejecuta el comando erase startup-config y todavía no se ha apagado/reiniciado el router se puede recuperar la configuración, ya que aunque la NVRAM está vacía la RAM todavía contiene la información, para restaurarla, ejecutar el comando copy running-config startup-config..

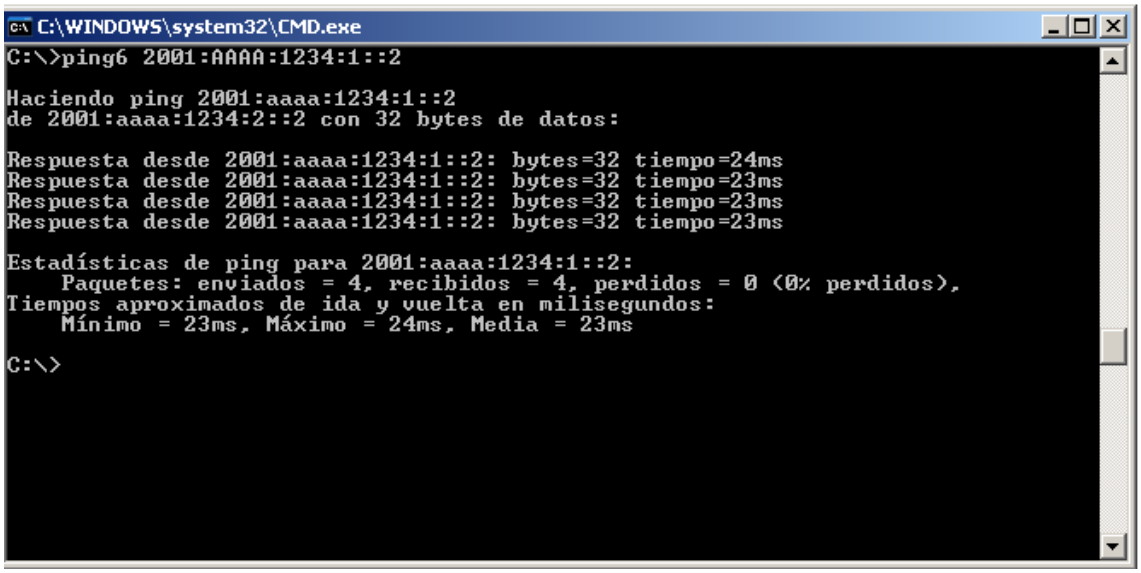
ANEXO D

VERIFICACION DE CONECTIVIDAD ENTRE HOSTS Y ROUTERS

1._ Conectividad entre los Host A al Host B

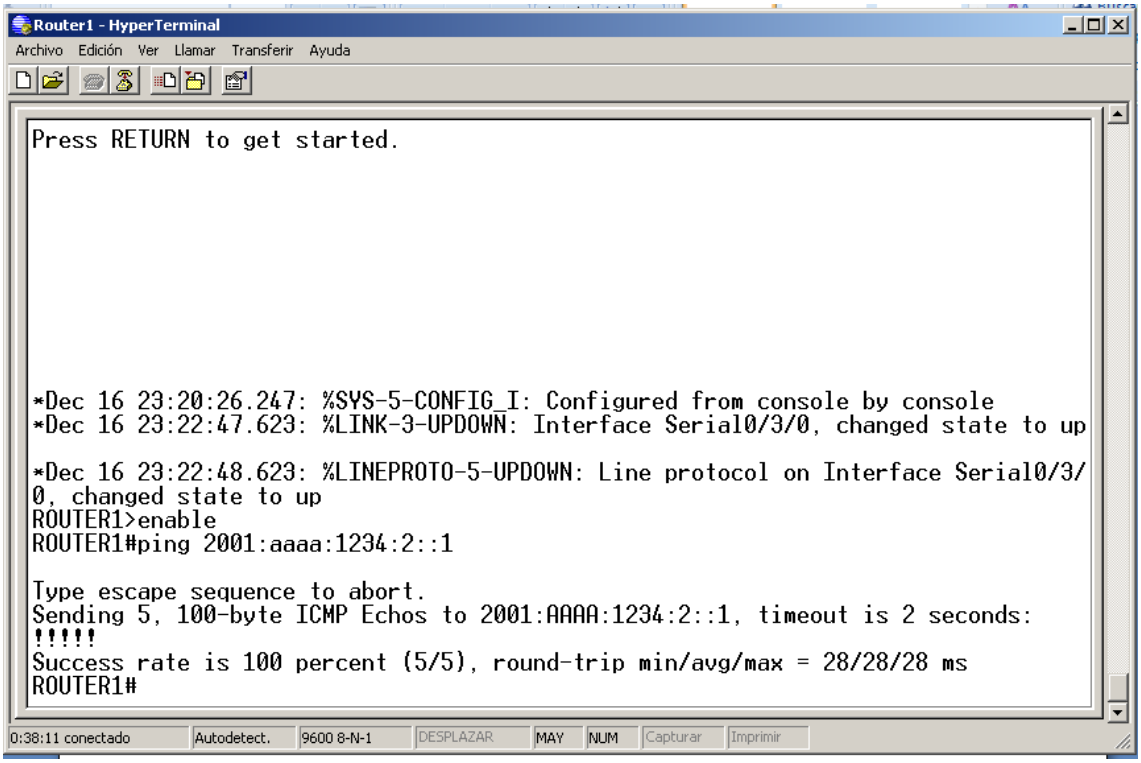


2._ Conectividad entre los Host B al Host A

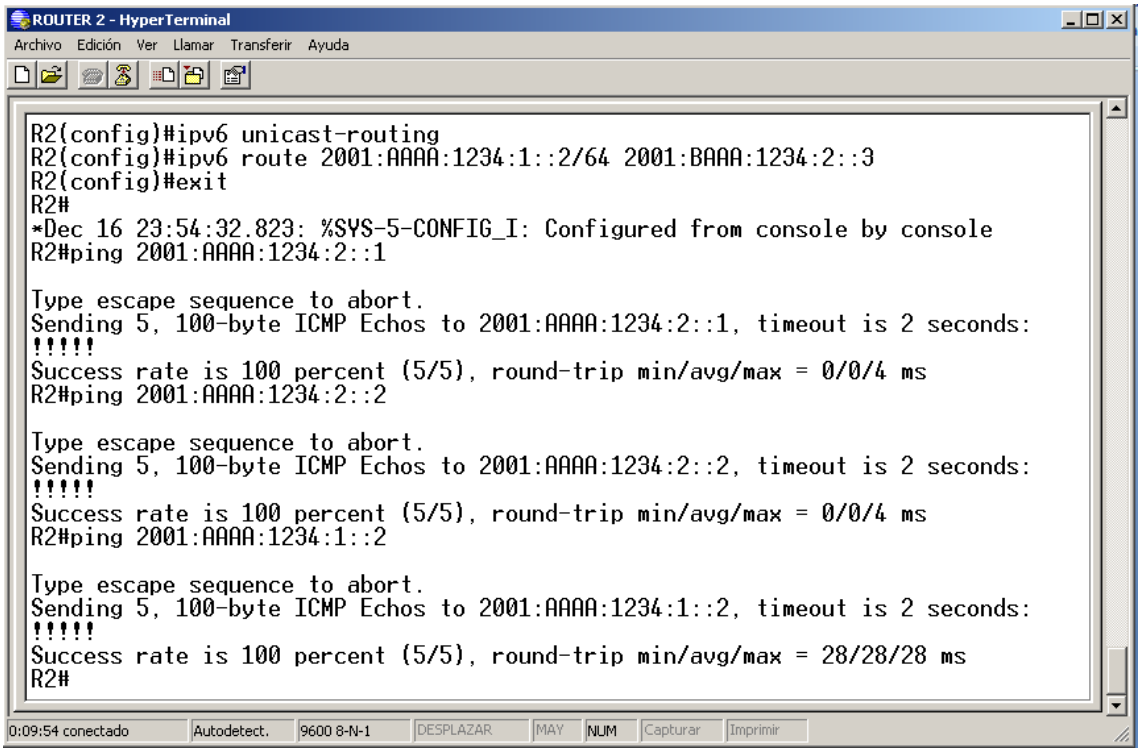


3._ Conectividad entre los Routers al Host

Router 1 al Router 2



Router 2 hace ping a todos los puntos de conectividad

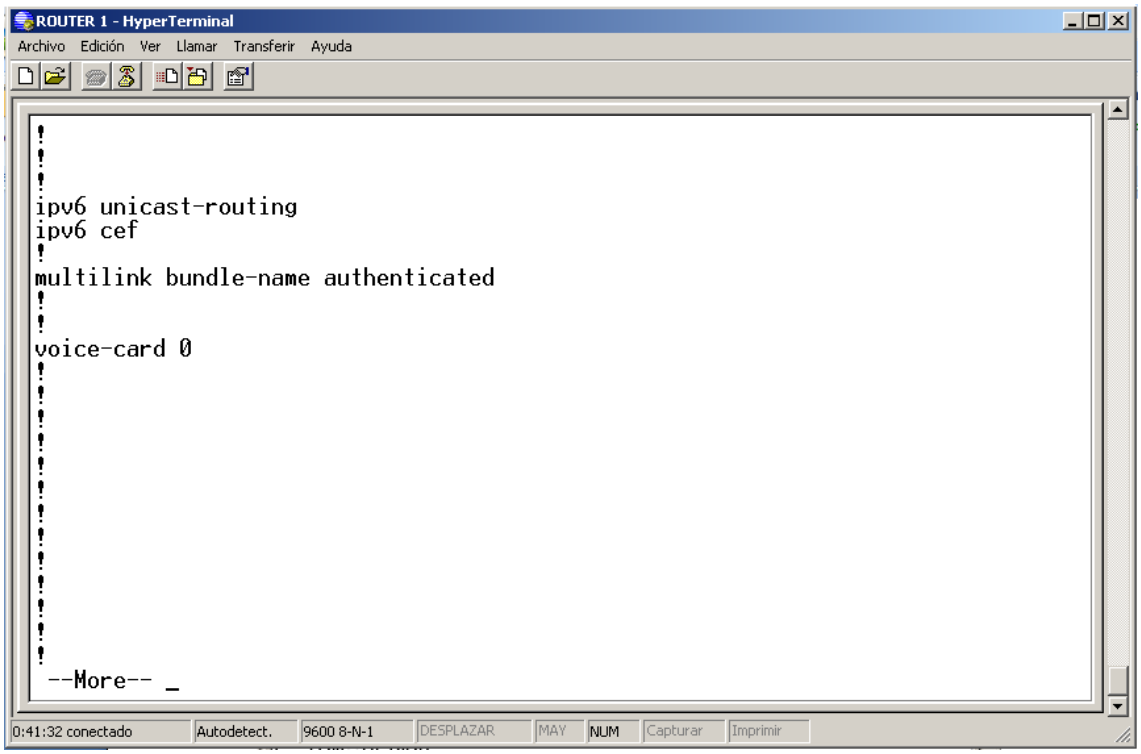


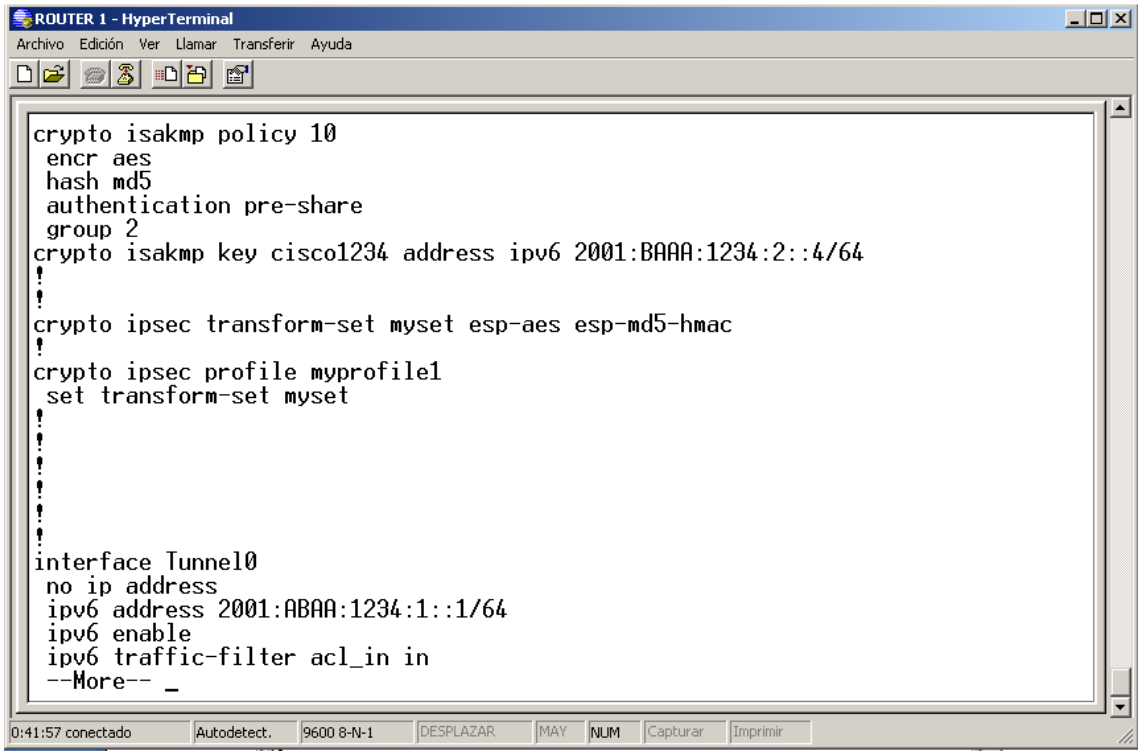
ANEXO E

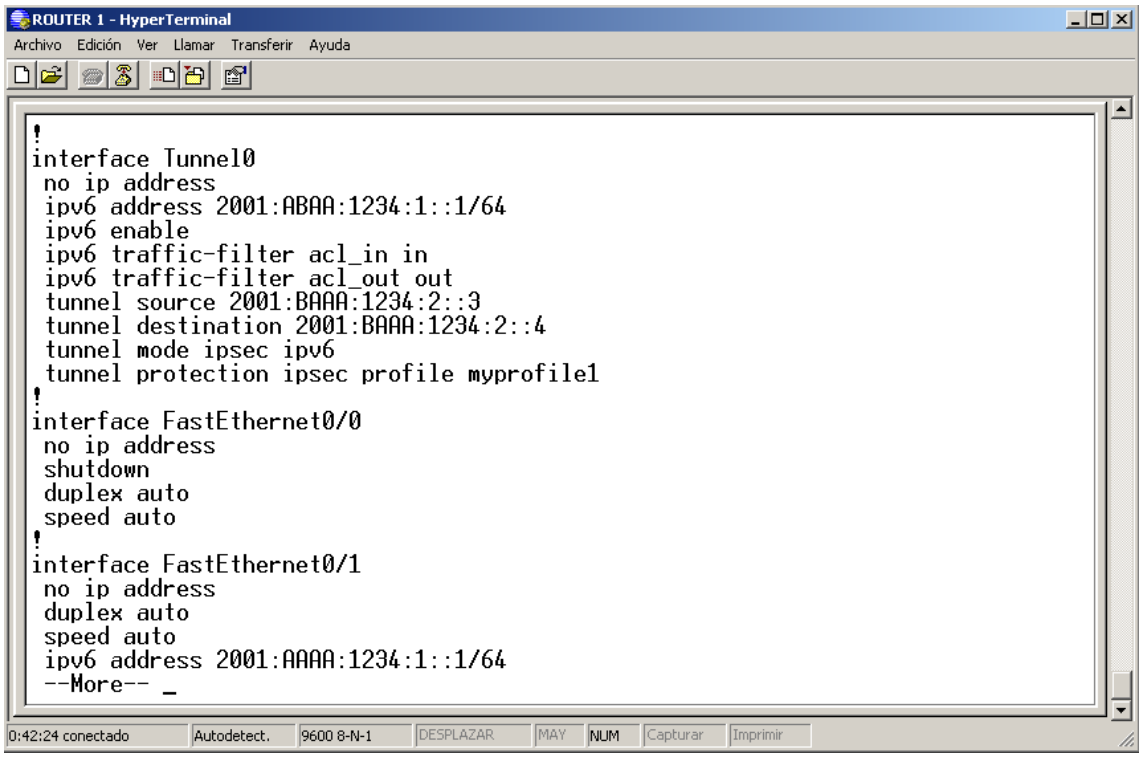
DETALLES DE CONECTIVIDAD MEDIANTE EL COMANDO SHOW

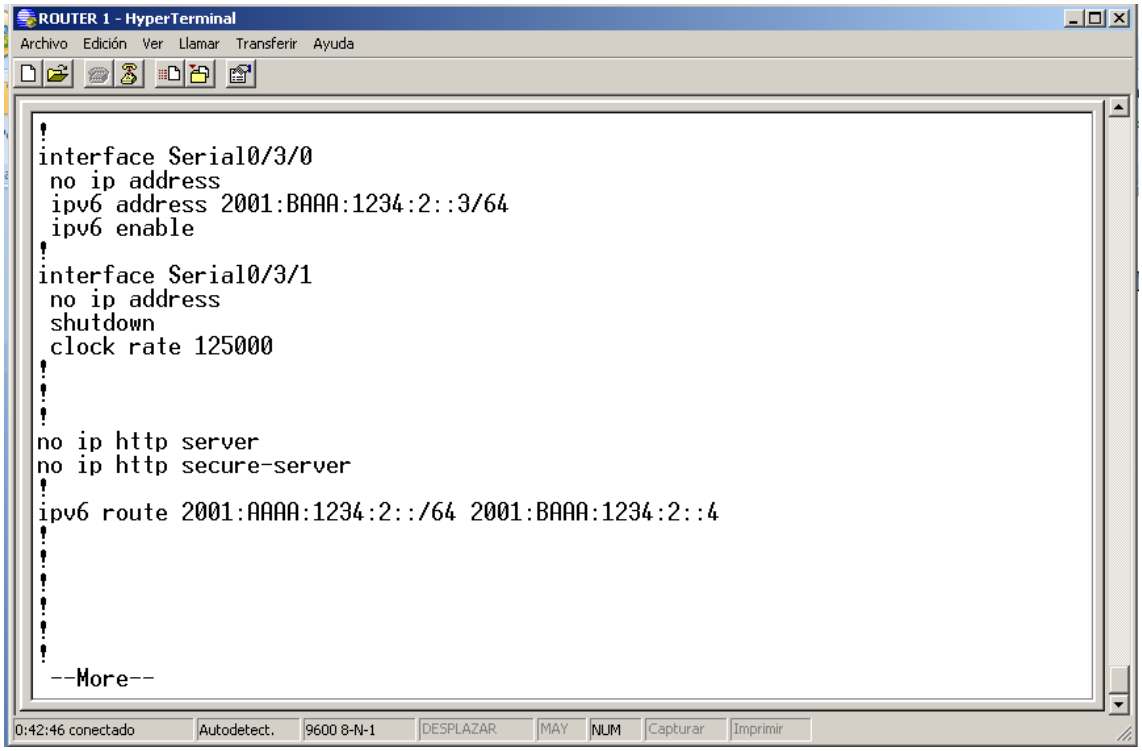
1:_ SHOW RUNNING CONFIG

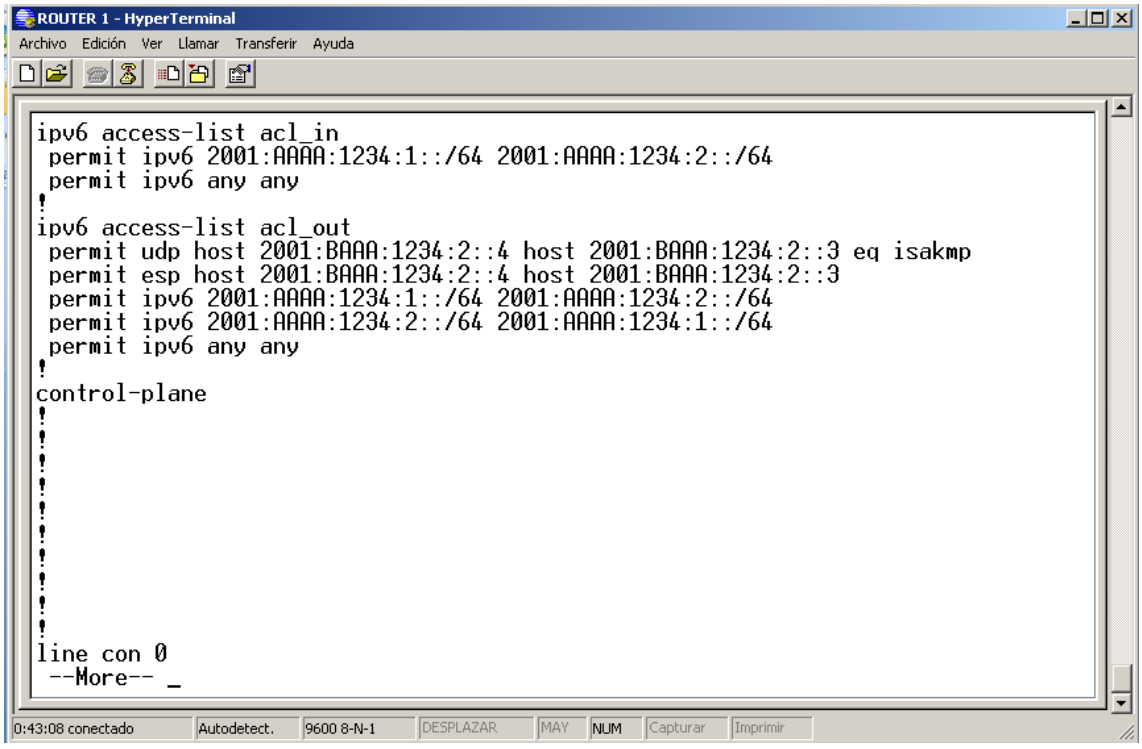
Router 1



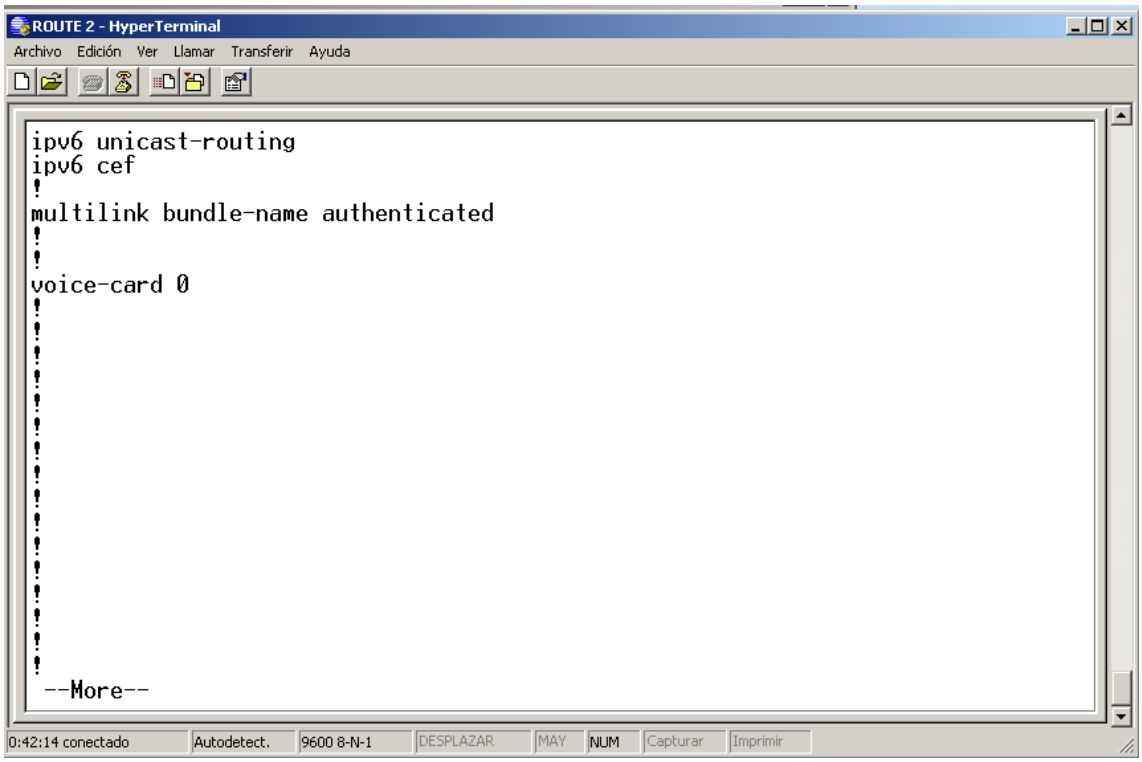

ROUTER 1 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
crypto isakmp policy 10
encr aes
hash md5
authentication pre-share
group 2
crypto isakmp key cisco1234 address ipv6 2001:BAAA:1234:2::4/64
!
!
crypto ipsec transform-set myset esp-aes esp-md5-hmac
!
crypto ipsec profile myprofile1
set transform-set myset
!
!
!
!
!
!
interface Tunnel0
no ip address
ipv6 address 2001:ABAA:1234:1::1/64
ipv6 enable
ipv6 traffic-filter acl_in in
--More-- _
0:41:57 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir

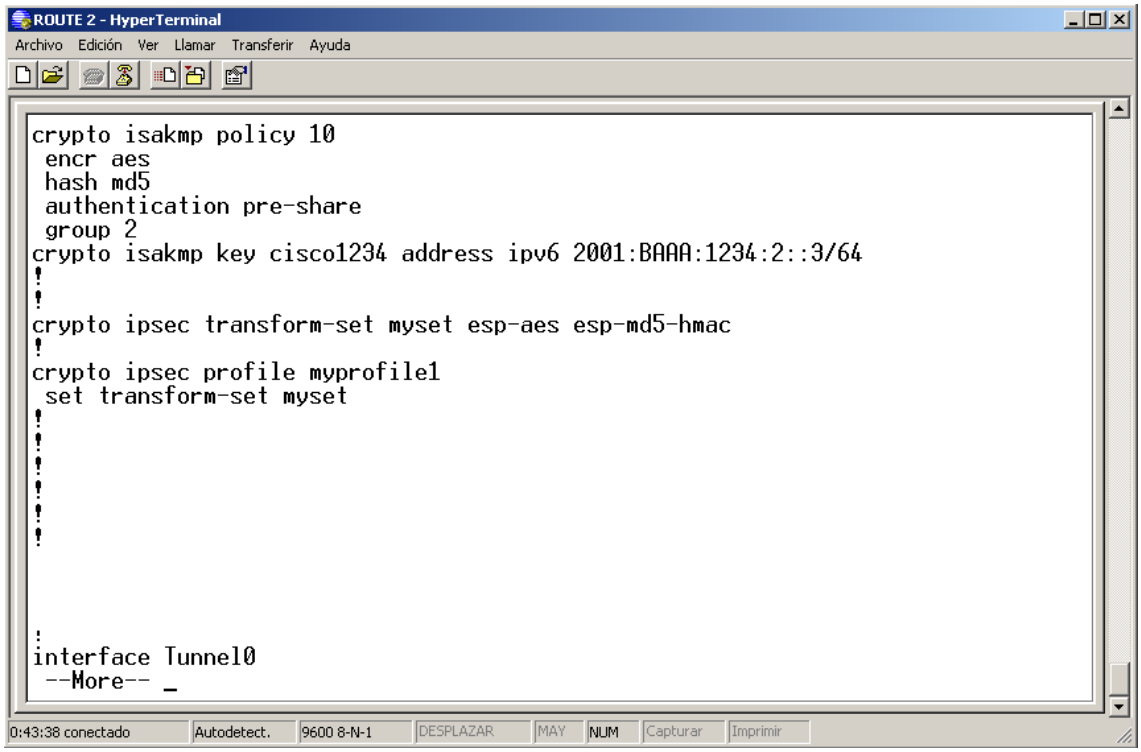

ROUTER 1 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
!
interface Tunnel0
no ip address
ipv6 address 2001:ABAA:1234:1::1/64
ipv6 enable
ipv6 traffic-filter acl_in in
ipv6 traffic-filter acl_out out
tunnel source 2001:BAAA:1234:2::3
tunnel destination 2001:BAAA:1234:2::4
tunnel mode ipsec ipv6
tunnel protection ipsec profile myprofile1
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
ipv6 address 2001:AAAA:1234:1::1/64
--More-- _
0:42:24 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir

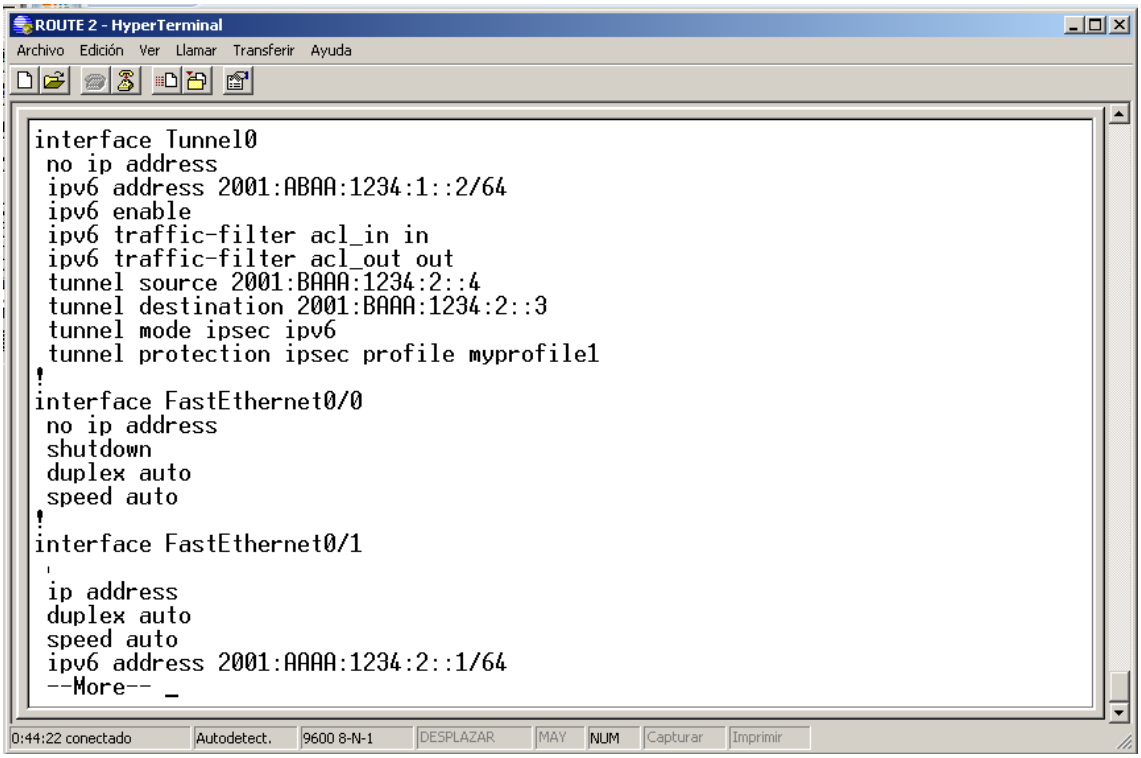

ROUTER 1 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
!
interface Serial0/3/0
 no ip address
 ipv6 address 2001:BAAA:1234:2::3/64
 ipv6 enable
!
interface Serial0/3/1
 no ip address
 shutdown
 clock rate 125000
!
!
!
no ip http server
no ip http secure-server
!
ipv6 route 2001:AAAA:1234:2::/64 2001:BAAA:1234:2::4
!
!
!
!
!
 --More--
0:42:46 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir

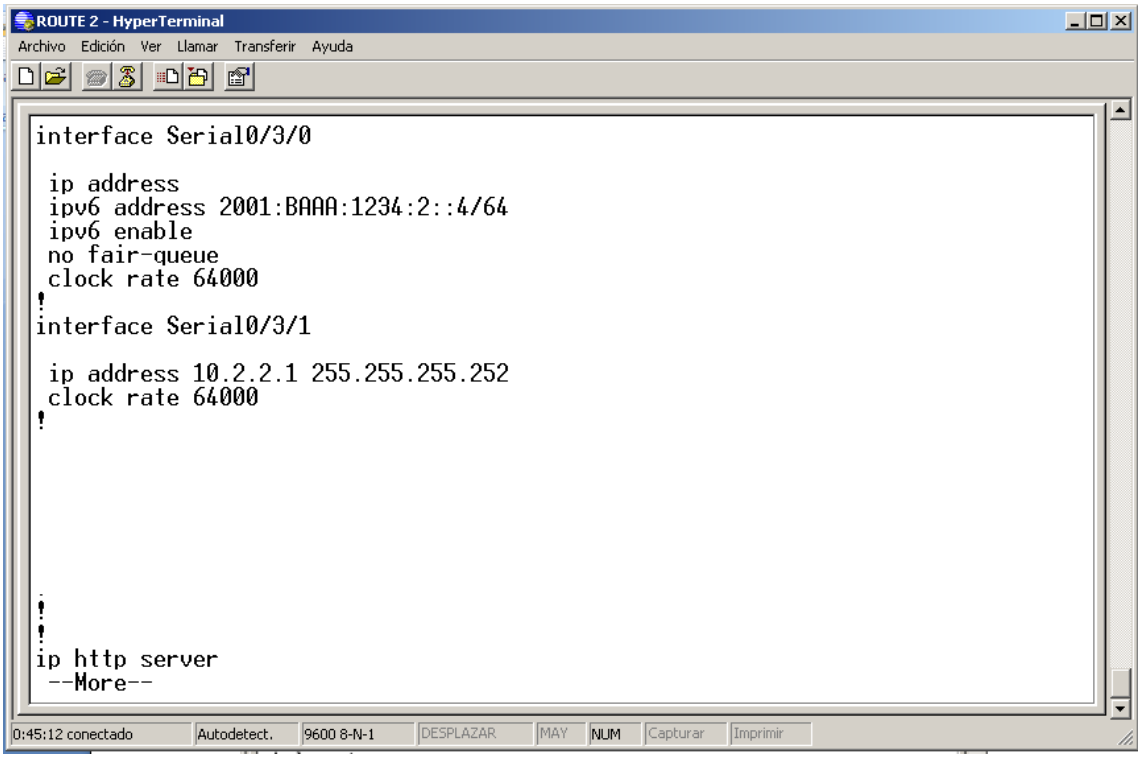

ROUTER 1 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
ipv6 access-list acl_in
 permit ipv6 2001:AAAA:1234:1::/64 2001:AAAA:1234:2::/64
 permit ipv6 any any
!
ipv6 access-list acl_out
 permit udp host 2001:BAAA:1234:2::4 host 2001:BAAA:1234:2::3 eq isakmp
 permit esp host 2001:BAAA:1234:2::4 host 2001:BAAA:1234:2::3
 permit ipv6 2001:AAAA:1234:1::/64 2001:AAAA:1234:2::/64
 permit ipv6 2001:AAAA:1234:2::/64 2001:AAAA:1234:1::/64
 permit ipv6 any any
!
control-plane
!
!
!
!
!
!
!
!
!
!
line con 0
 --More-- _
0:43:08 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir

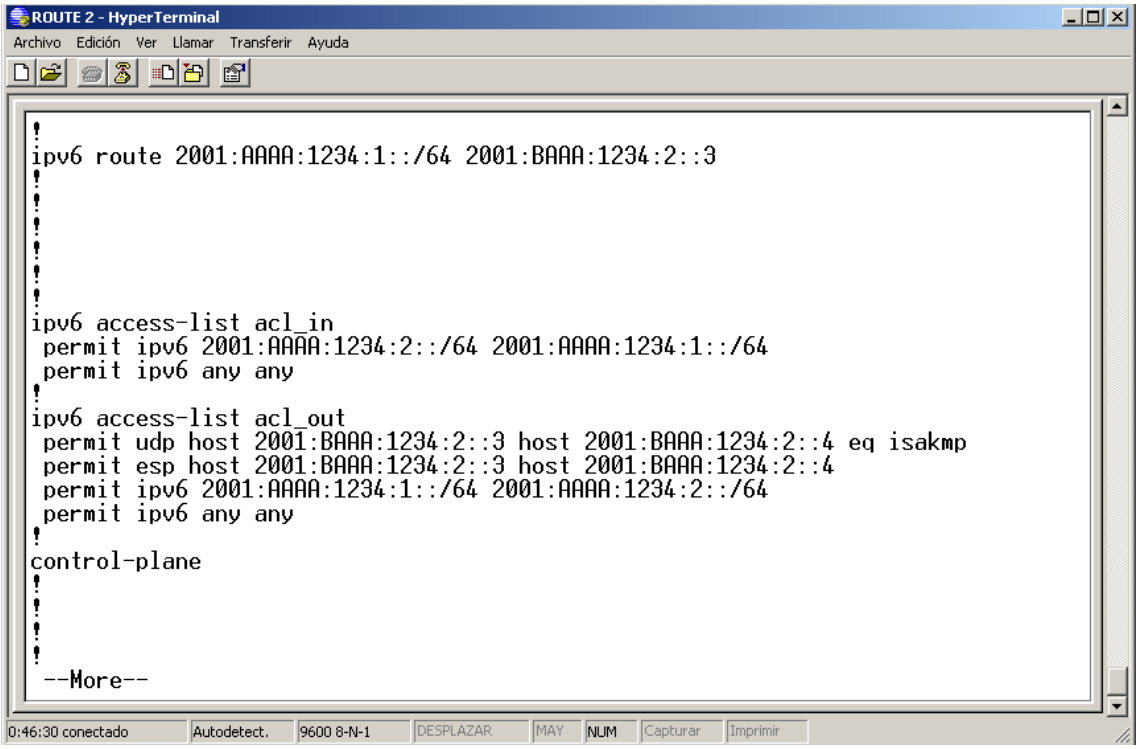
Router 2


ROUTE 2 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
ipv6 unicast-routing
ipv6 cef
!
multilink bundle-name authenticated
!
!
voice-card 0
!
!
!
!
!
!
!
!
!
!
!
!
!
!
--More--
0:42:14 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir


ROUTE 2 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
crypto isakmp policy 10
encr aes
hash md5
authentication pre-share
group 2
crypto isakmp key cisco1234 address ipv6 2001:BAAA:1234:2::3/64
!
!
crypto ipsec transform-set myset esp-aes esp-md5-hmac
!
crypto ipsec profile myprofile1
set transform-set myset
!
!
!
!
!
!
!
interface Tunnel0
--More-- _
0:43:38 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir

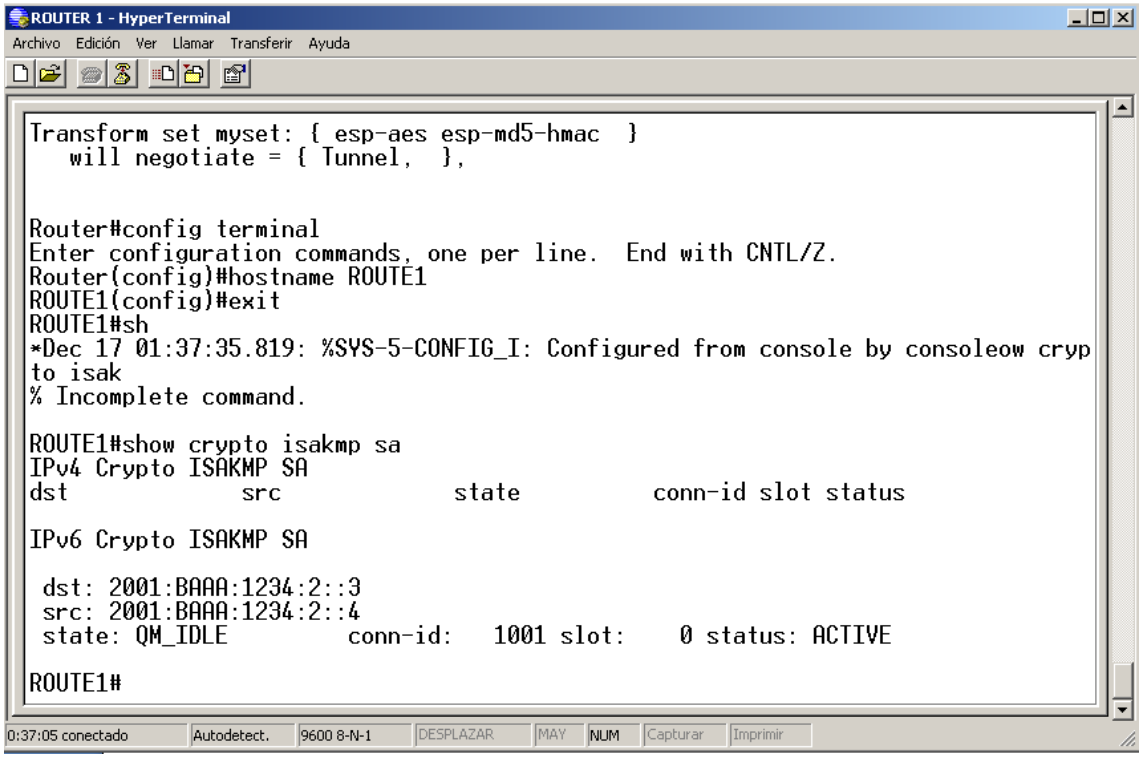

ROUTE 2 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
interface Tunnel0
no ip address
ipv6 address 2001:ABAA:1234:1::2/64
ipv6 enable
ipv6 traffic-filter acl_in in
ipv6 traffic-filter acl_out out
tunnel source 2001:BAAA:1234:2::4
tunnel destination 2001:BAAA:1234:2::3
tunnel mode ipsec ipv6
tunnel protection ipsec profile myprofile1
!
interface FastEthernet0/0
no ip address
shutdown
duplex auto
speed auto
!
interface FastEthernet0/1
ip address
duplex auto
speed auto
ipv6 address 2001:AAAA:1234:2::1/64
--More-- _
0:44:22 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir


ROUTE 2 - HyperTerminal
Archivo Edición Ver Llamar Transferir Ayuda
interface Serial0/3/0
ip address
ipv6 address 2001:BAAA:1234:2::4/64
ipv6 enable
no fair-queue
clock rate 64000
!
interface Serial0/3/1
ip address 10.2.2.1 255.255.255.252
clock rate 64000
!
!
!
ip http server
--More--
0:45:12 conectado
Autodetect.
9600 8-N-1
DESPLAZAR
MAY
NUM
Capturar
Imprimir

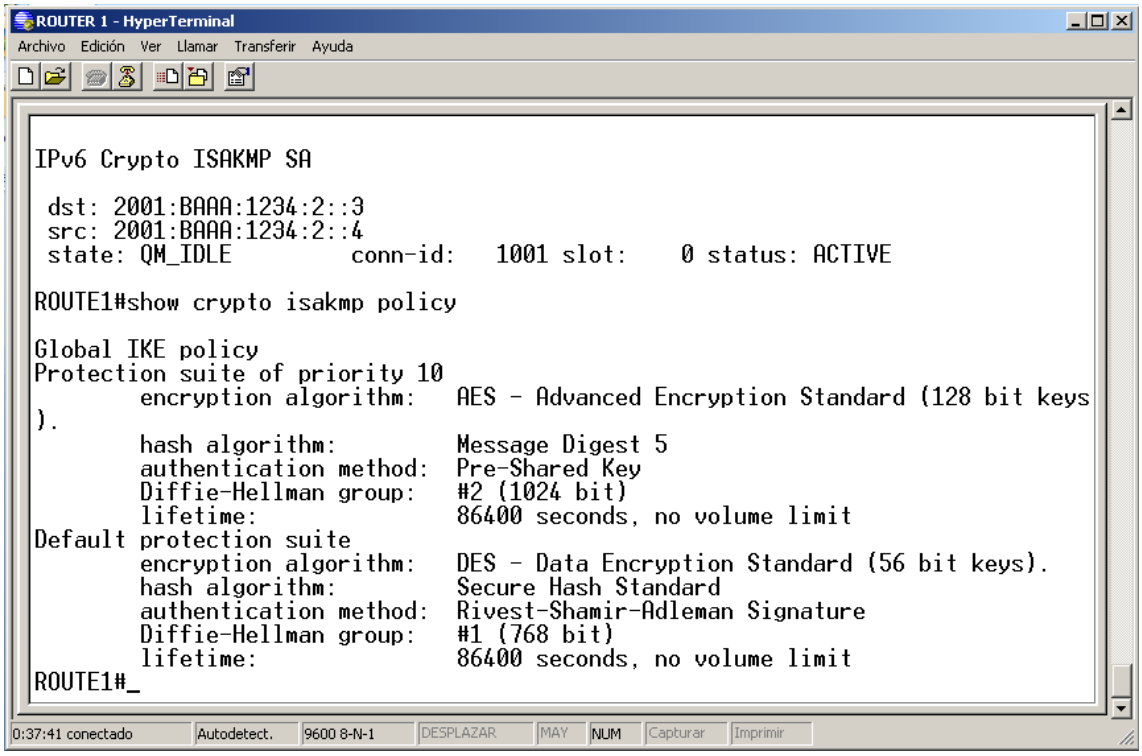


2:_ SHOW CRYPTO ISAKMP SA

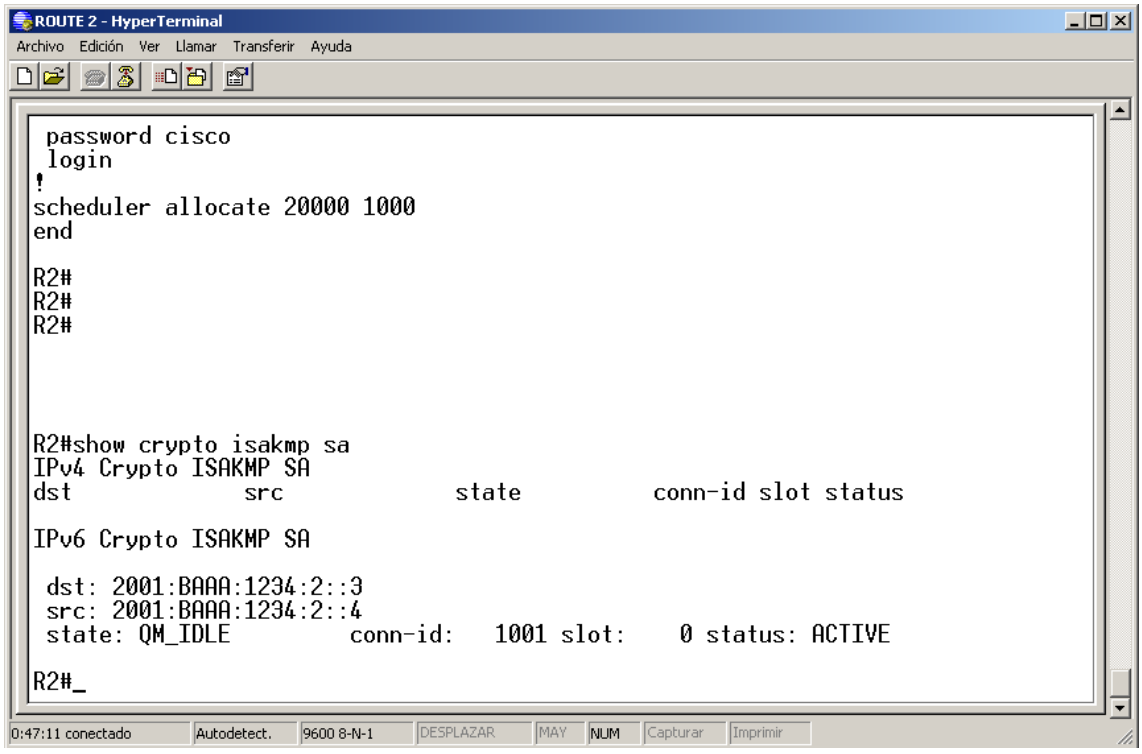
Router 1



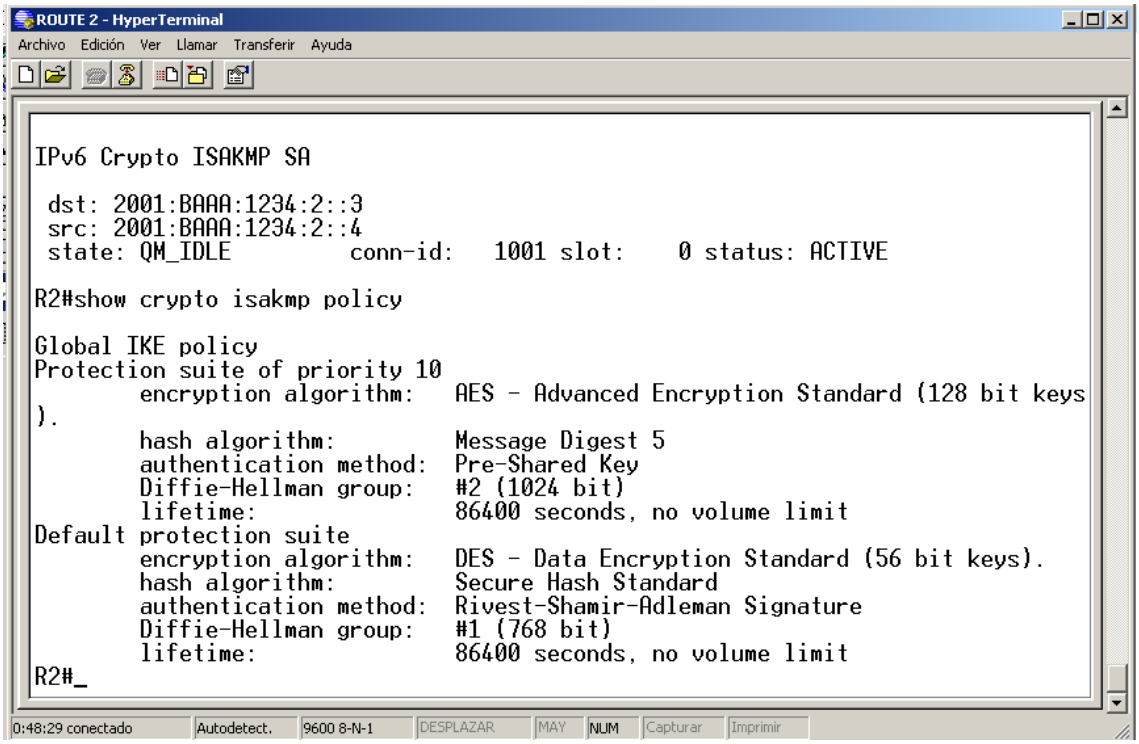
Show crypto isakmp policy



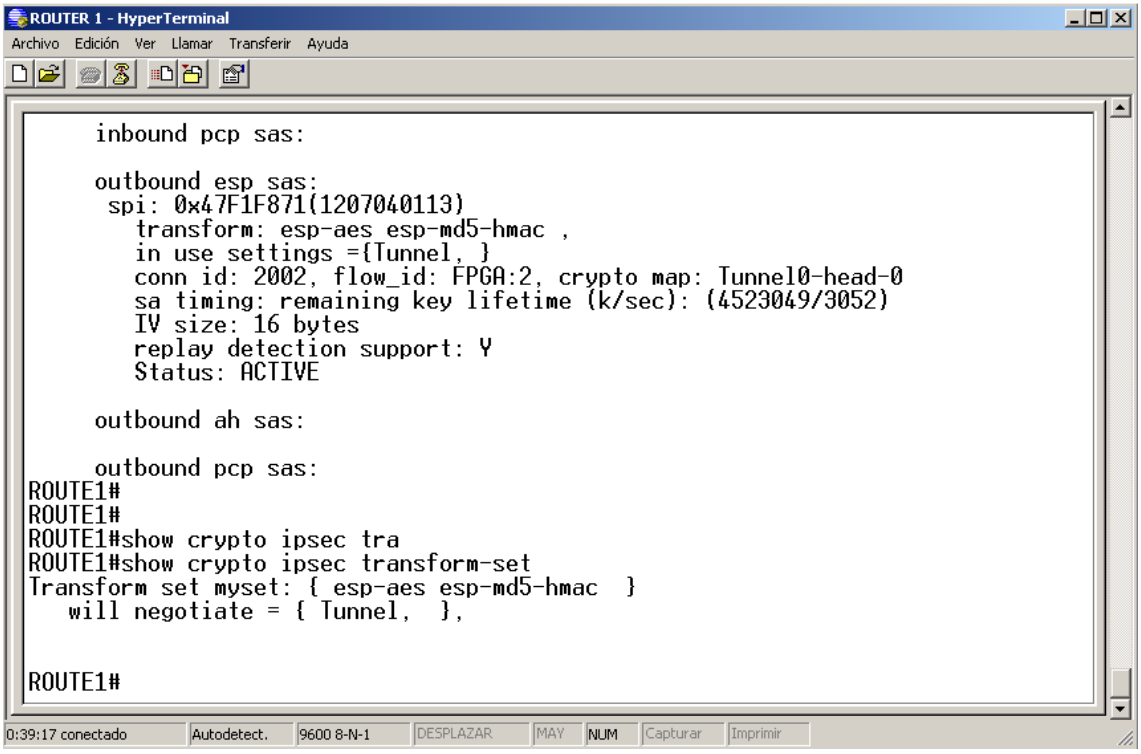
Router 2



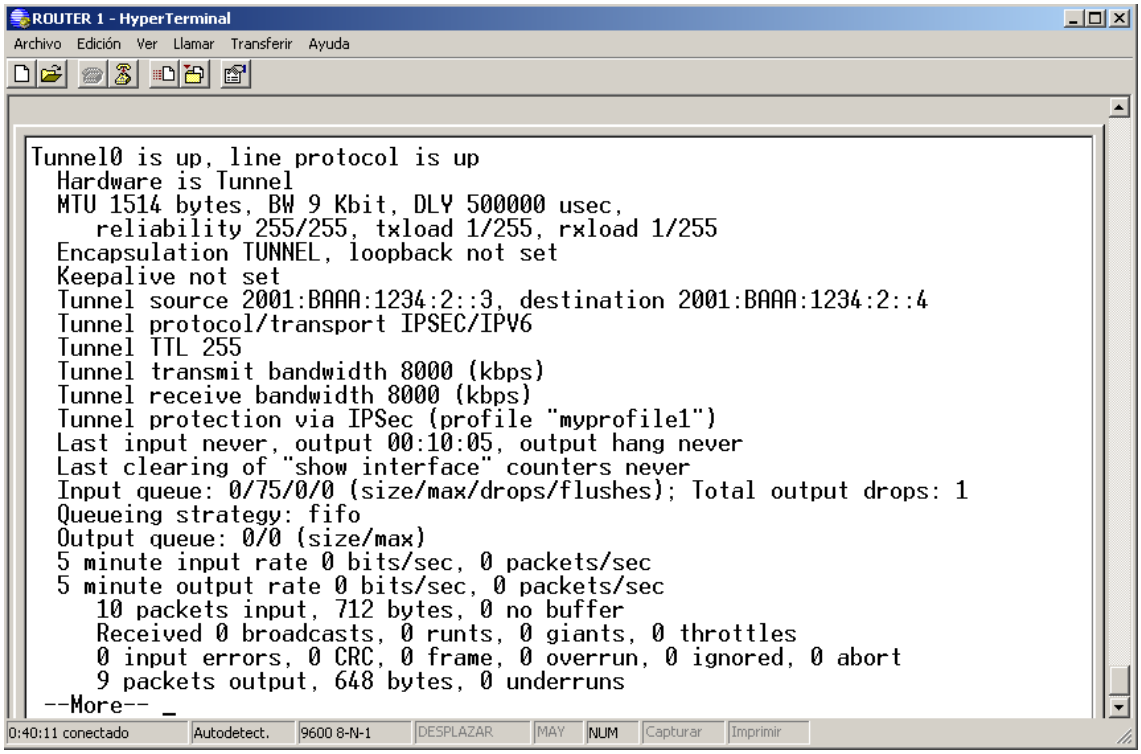
Show crypto isakmp policy



3:_ SHOW CRYPTO IPSEC TRANSFORM-SET



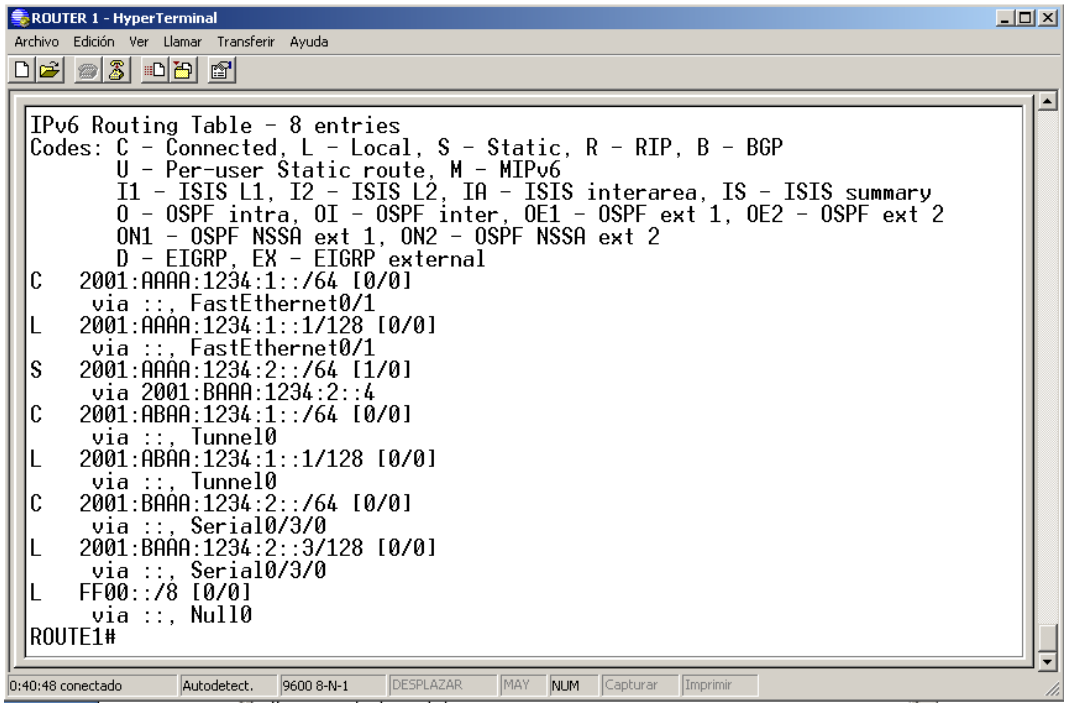
4:_ SHOW CRYPTO TUNNEL



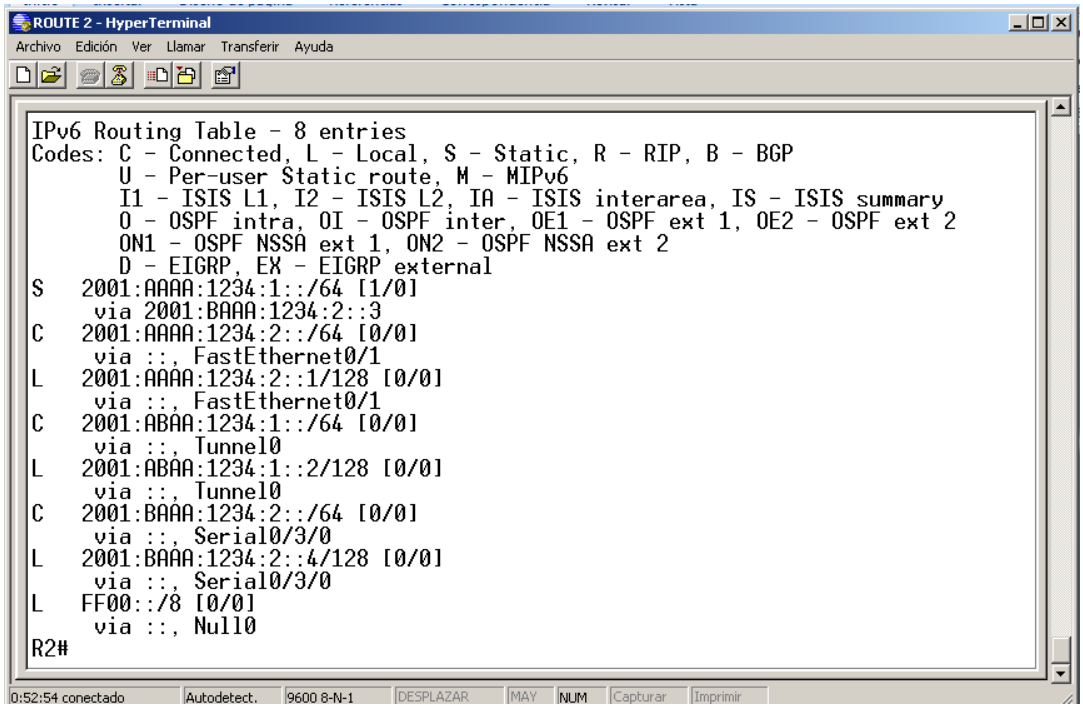
ANEXO D

DETALLES DE LAS RUTAS ESTATICAS

Router 1



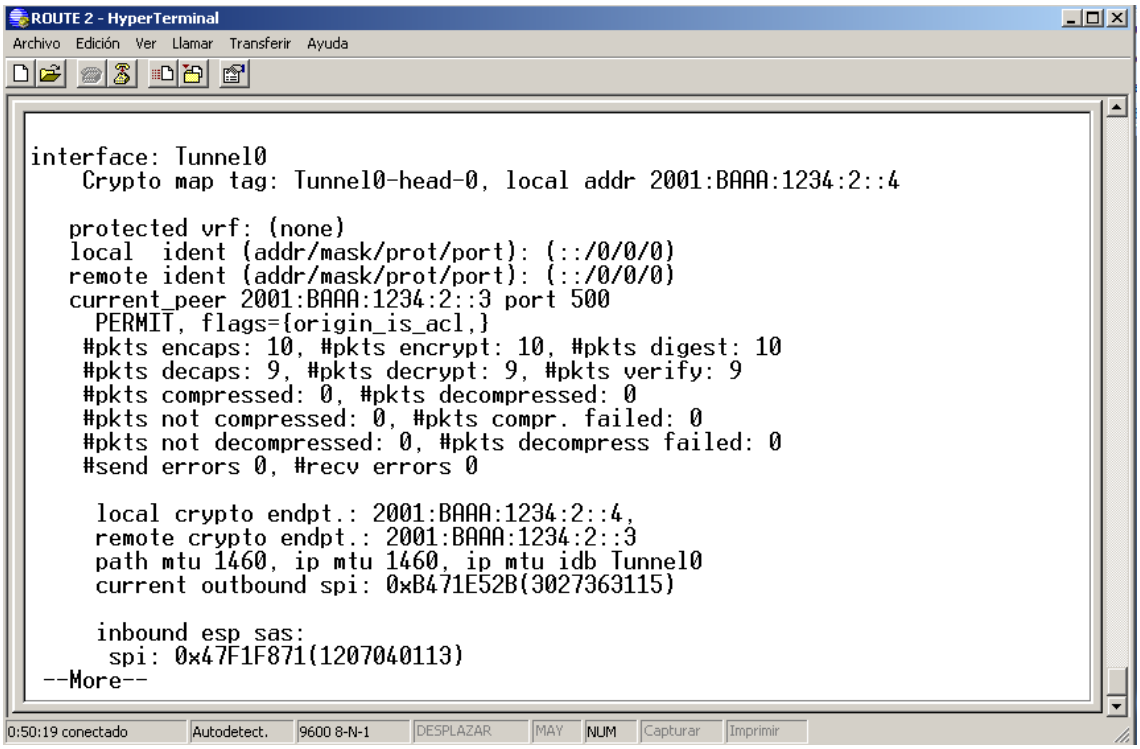
Router 2

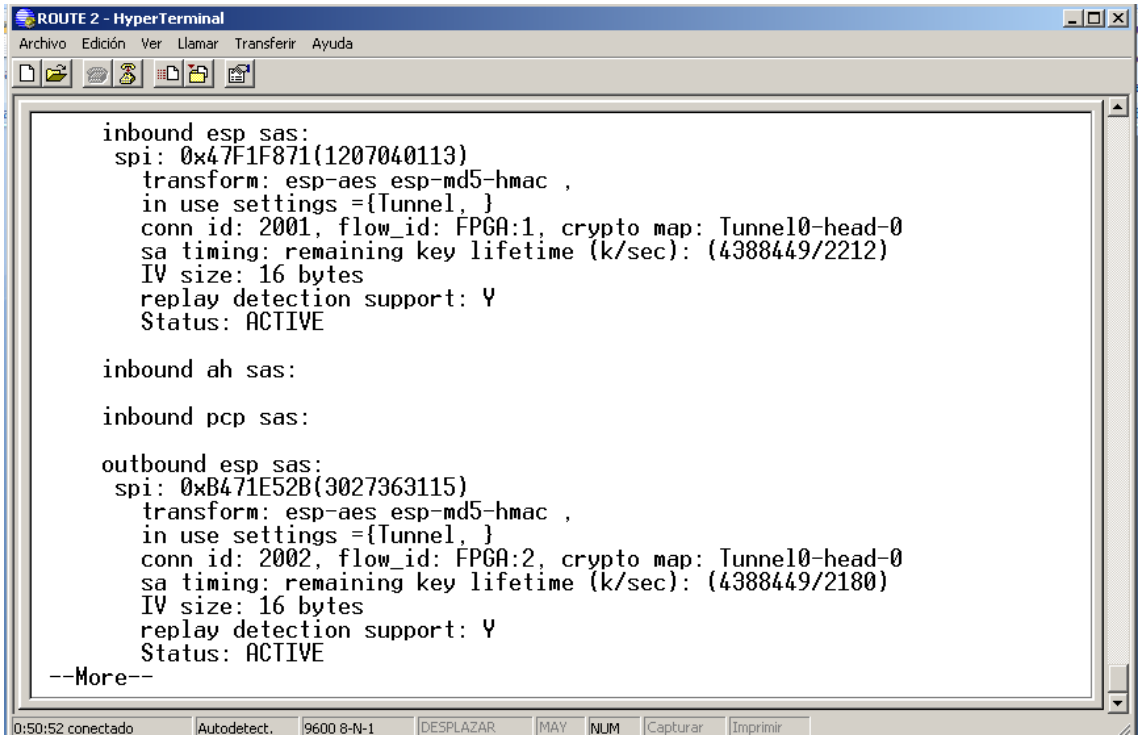


ANEXO E

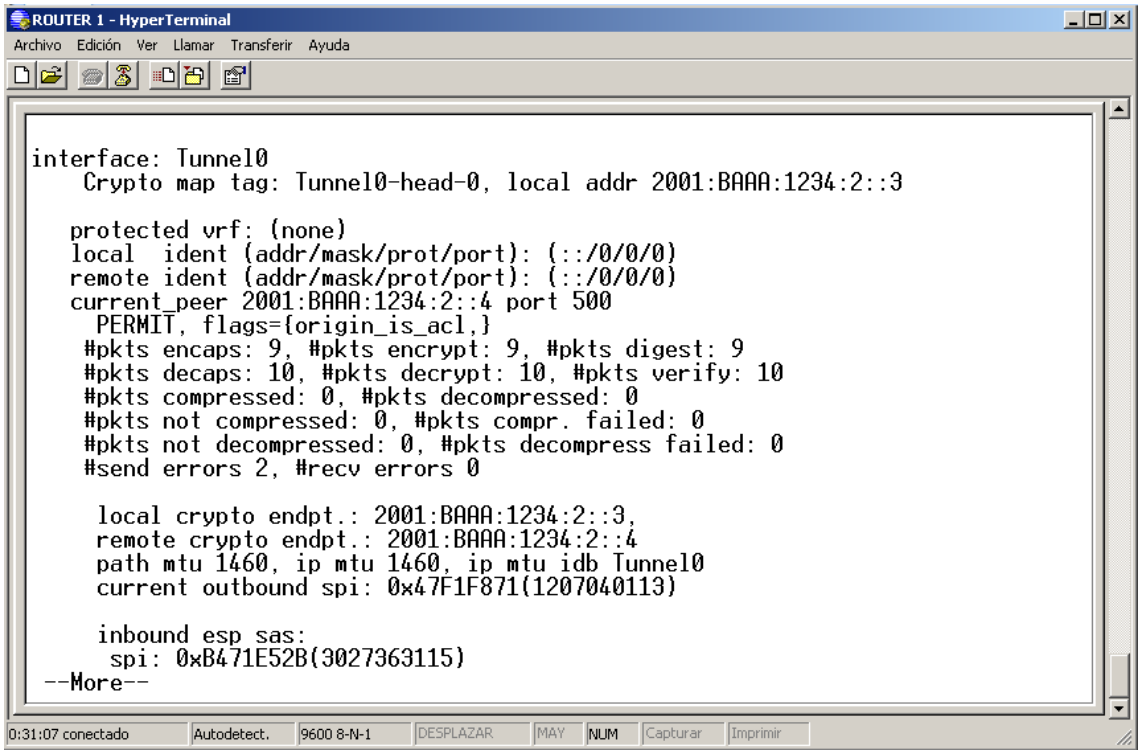
COMPROBACION DE PAQUETES ENCRYPTADOS

Router 2





Router 1



Se genera error en uno de los routers porque los primeros paquetes se pierden cuando fenece la TTL del paquete en el proceso de la creación de la VPN, mientras más nodos se tenga se demora en establecer en túnel.