
# ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

**FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN**

"Implementación y pruebas de Simulación de una Red WAN-Cisco IPv6 para una institución Bancaria, utilizando SNMPv3 en su gestión"

## EXAMEN COMPLEXIVO

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

**INGENIERO EN ELECTRONICA Y TELECOMUNICACIONES**

Presentado por:

CARLOS FERNANDO NAVARRETE MARTÍNEZ
MARCO ANTONIO ALEJANDRO MORÁN

Guayaquil – Ecuador

AÑO 2015

# AGRADECIMIENTO

Agradezco a Dios por sus bendiciones y permitir que cumpla todas mis metas; a mis padres Beatriz Martínez y Marcos Navarrete por todo el esfuerzo y el amor que me han dado para seguir adelante y poder obtener un título profesional, a mis hijos por su constante apoyo, por estar siempre conmigo y ayudarme a superar cada día y a mis profesores por sus enseñanzas académicas.

**Carlos F. Navarrete M.**

Agradezco a mis padres por no dejar de confiar en mí y por su cariño, lo que me ha confortado en el trayecto de mi vida; a mis familiares que de una u otra manera me han brindado su apoyo. A todos mis maestros que me han enseñado lo necesario y han guiado en cuanto he necesitado.

**Marco A. Alejandro M.**

# DEDICATORIAS

Dedico este trabajo a Dios; a mi Madre por su comprensión y por todo su apoyo incondicional; a mis hijos, Ericka Adriana y Carlos; por la confianza depositada en mí, por siempre darme fuerzas para seguir adelante y por ser la razón de mi vida.

**Carlos F. Navarrete M.**

Dedico el presente a Dios por su amor y poder, que hizo posible que esté presente en este momento, a mis padres Medardo Alejandro y Rebeca Moran por su apoyo incondicional, buen ejemplo y principios, a mis hermanos y amigos que he ganado a lo largo de estos años, y a mis profesores por la excelente formación académica adquirida.

**Marco A. Alejandro M.**

# TRIBUNAL DE SUSTENTACIÓN

_____

M. Sc. Sara Ríos Orellana

**PRESIDENTA**

_____

Mg. Washington Medina Moreira

**DIRECTOR**

_____

Ph. D. Freddy Villao Quezada

**VOCAL**

# DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Grado, nos corresponde exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL" (Reglamento de Graduación de la ESPOL).

Carlos Fernando Navarrete Martínez

Marco Antonio Alejandro Moran

# RESUMEN

El presente proyecto se enfoca en la implementación de una infraestructura Bancaria, con el objetivo de preservar la información que se transmita a través de sus canales de comunicación con el uso del protocolo IPsec que es obligatorio en el nuevo protocolo de internet IPv6 y lograr gestionar esta infraestructura Bancaria en un ambiente seguro.

El capítulo uno trata sobre las características del protocolo de Internet IPv6, formato de su datagrama, algoritmos de enrutamiento, configuración automática y la seguridad del protocolo IPv6 sustentada en IPsec.

El capítulo dos detalla el modelo de Gestión de Red, arquitectura del Protocolo SNMP y se detalla el Protocolo SNMPv3. El fundamento teórico está basado en RFC`s que sustentan su operación.

El capítulo tres detalla la configuración de la red Bancaria, la topología, el modelo de direccionamiento en IPv6, el enrutamiento OSPFv3, el diseño de seguridad de enrutadores y la elección de la aplicación de Gestión de Red en el servidor NMS.

En el capítulo cuatro se seleccionó el software de simulación GNS3, son implementados los enrutadores Cisco con sus respectivas direcciones IPv6, además se establece los parámetros de Autenticación y Encriptación de los enlaces entre enrutadores y se indican las comunidades de monitoreo SNMPv1, SNMPv2 y en la versión SNMPv3 se agrega el usuario y clave de monitoreo.

Se Implementa el servidor de monitoreo NMS, se realiza el análisis de tráfico en nuestras interfaces, con lo cual se muestra las diferencias que hay entre los protocolos SNMPv1, SNMPv2c y SNMPv3.

En el capítulo cinco se realiza el análisis de costos para implementar dicha infraestructura.

El objetivo principal del presente trabajo es mostrar que, con el uso de del protocolo IPv6 y la utilización de IPsec se podría asegurar la integridad y la confidencialidad de la información que se transmite a través de la red de datos. La gestión de la infraestructura pueda ser implementada con el uso de SNMPv3 y lograr una administración segura de la infraestructura.

# ÍNDICE GENERAL

# ABREVIATURAS

| | |
|---|---|
| IP: | Internet Protocol o Protocolo de Internet. |
| IPv4: | Internet Protocol versión 4 o Protocolo de Internet versión 4. |
| IPv6: | Internet Protocol versión 6 o Protocolo de Internet versión 6. |
| IETF: | Internet Engineering Task Force o Fuerza de Tareas de Ingeniería de Internet. |
| RFC: | Request for Comments o Petición de comentarios. |
| IPng: | Internet Protocol next generation o Siguiente generación de Protocolo de Internet. |
| IPsec: | Internet Protocol security o Protocolo de Seguridad de Internet. |
| QoS: | Quality of Service o Calidad de Servicio. |
| ISO: | International Organization for Standardization o Organización Internacional de Normalización. |
| OSI: | Open System Interconnection o Modelo de Interconexión de sistemas abiertos. |
| Plug&Play: | Plug-and-Play o Enchufar y usar. |
| ICMPv6: | Internet Control Message Protocol versión 6 o Protocolo de Mensajes de Control de Internet. |
| UDP: | User Datagram Protocol |
| ND: | Neighbor Discovery |

| | |
|---|---|
| DNS: | Domain Name System |
| SNMP: | Simple Network Manager Protocol |
| RDSI: | Red Digital Servicios Integrados |
| GSM: | Global System for Mobile Communications |
| TMN: | Telecommunications Management Network |
| ITU-T: | International Telecommunication Union |
| CCITT: | Consultative Committee for International Telegraphy and Telephony |
| OSI: | Open System Interconnection |
| NMS: | Network Management Systems |
| MIB: | Management Information Base |
| SNMPv1: | Simple Network Manager Protocol Version 1 |
| SNMPv2: | Simple Network Manager Protocol Version 2 |
| SNMPv3: | Simple Network Manager Protocol Version 3 |
| PDU: | Unidades de Datos de Protocolo |
| USM: | Modelos de Seguridad de Usuario |
| NRC: | Non recurring charge |
| MRC: | Monthly recurring Charge |

# ÍNDICE DE FIGURAS

# ÍNDICE DE TABLAS

# INTRODUCCIÓN

La importancia del Protocolo de Internet Versión Seis (IPv6 por sus siglas en inglés) ha tomado fuerza en los últimos tiempos por el asunto de la cantidad de IPs públicas, ya que en la anterior versión (IPv4) están agotadas; en esta nueva versión del protocolo, se tomó en cuenta el crecimiento del Internet así como también la seguridad.

El objetivo del presente trabajo es presentar las bondades del Protocolo de Internet versión seis (IPv6 por sus siglas en inglés) con el conjunto de Protocolos de Seguridad de Internet (IPsec por sus siglas en inglés) habilitados en la comunicación de una Red de Área Amplia (WAN) piloto de una Institución Bancaria y la administración de la misma a través del Protocolo Simple de Administración de Red versión tres (SNMPv3 – Por sus siglas en inglés) desde un servidor de Gestión de Red.

Para obtener los objetivos se realizará el diseño de una Red Bancaría Piloto con todos los elementos de Red y seguridad que intervienen. Se analizarán esquemas de Redes existentes y se propondrá mejoras, luego se implementará una Red de área Amplia (WAN) piloto con IPv6 en cada uno de sus elementos activos.

Se analizará cuál es el mejor software de Gestión de red con herramientas de Open Source tales como JFFNMS, CACTI o NAGIOS, también con software de Gestión de Red Propietarios como HP–Openview, y Solarwinds Orion NPM. Luego de instalarlo se analizará la información recopilada en el Servidor de Gestión de Red con SNMPv3.

Los resultados esperados al finalizar el presente trabajo, es que la simulación de la administración del servidor de gestión y los Equipos en la WAN no sufre degradación al usar el Stack de IPv6.

Se debe demostrar que los datos viajan encriptados mediante la utilización del conjunto de protocolos IPSEC en IPv6, así como el Sistema Operativo de los enrutadores debe soportar los protocolos mencionados anteriormente.

# CAPÍTULO 1

## 1 PROTOCOLO DE INTERNET VERSIÓN 6 (IPV6)

### 1.1 Características del Protocolo de Internet versión 6 (IPv6)

La actual versión del protocolo de internet IPv4, es flexible y muy potente, pero actualmente ya llegó a su nivel máximo de saturación; la poca cantidad de direcciones IPv4 disponibles, generará limitaciones al funcionamiento de las redes actuales y futuras. Este es el motivo básico por el que surge en el seno del IETF (Internet Engineering Task Force), el protocolo IPv6. Este nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generation), fue la respuesta a la evidente falta de direcciones IP.

El nuevo protocolo permite corregir deficiencias del protocolo IPv4 y aportará un nuevo esquema de direccionamiento, encriptación de datos, un esquema de seguridad basada en los protocolos IPSec (Internet Protocol Security), configuración automática, calidad de servicio; permitirá además tener una mayor velocidad y un óptimo desempeño, acorde con la evolución actual del internet.

Una de las características de esta nueva versión es el sistema de direcciones, o sea mayor espacio de direccionamiento. En la nueva versión IPv6 las direcciones IP se multiplican por cuatro y nos ofrece un espacio de $2^{128}$ (340.282.366.920.938.463.463.374.607.431.768.211.456) direcciones versus la actual versión IPv4 que tiene un espacio de direcciones de 32 bits asociados en 4 grupos de 8 bits, por lo que se podrían asignar $2^{32}$ (4.294.967.296) direcciones.

Sin embargo, IPv4 tiene otros problemas o “dificultades” que IPv6 soluciona o mejora.

Debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear “parches” al protocolo básico. Entre los

“parches” más conocidos, podemos citar medidas para permitir la calidad de Servicio (QoS), Seguridad (IPsec), y Movilidad, fundamentalmente.

### 1.1.1 Características principales de IPv6

[1] Las características fundamentales de IPv6:

- Mayor espacio de direcciones.
- “Plug & Play”: Configuración Automática.
- Seguridad Intrínseca en el núcleo del protocolo (IPsec).
- Calidad de Servicio (QoS).
- Multicast: Envió de UN mismo paquete a un Grupo de Receptores.
- Anycast: Envió de UN paquete a UN receptor dentro de UN Grupo.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los enrutadores.
- Posibilidad de paquetes con carga útil (datos) de más de 65.535 bytes.
- Encaminado más eficiente en el troncal (backbone) de la red, debido a una jerarquía de direccionamiento basada en la agregación.
- Remuneración que facilita el cambio de proveedor de servicios.
- Características de movilidad.

## 1.2 Datagrama del protocolo de Internet (IPv6)

El datagrama del protocolo IPv6 no ha sufrido grandes cambios con respecto al datagrama del protocolo IPv4; el datagrama IPv6 es más bien una evolución mejorada y optimizada del datagrama del protocolo IPv4.

Para obtener el datagrama IPv6, al datagrama IPv4, mostrado en la figura 1.1, se le suprimieron siete campos (tamaño de cabecera, tipo de servicio, número de identificación del datagrama, banderas, numero de byte del datagrama fragmentado, ckecksum, opciones), y se rediseñaron los campos de longitud del datagrama, tiempo de vida y tipo de protocolo.

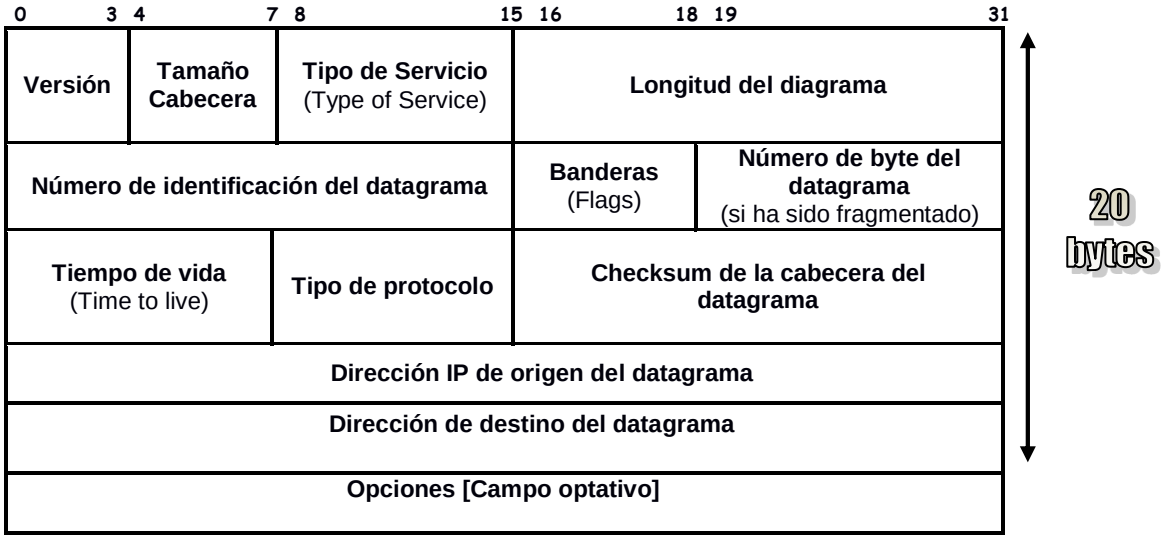



Figura 1.1 Datagrama IPv4 [3]

En el datagrama IPv6 como se muestra en la figura 1.2, se renombró algunos campos:

- Longitud del diagrama por Tamaño de los datos.
- Tiempo de vida por Límite de saltos.
- Protocolo por Siguiente cabecera.

Los nuevos campos que se incorporan son:

- Clase de trafico
- Etiqueta de Flujo.

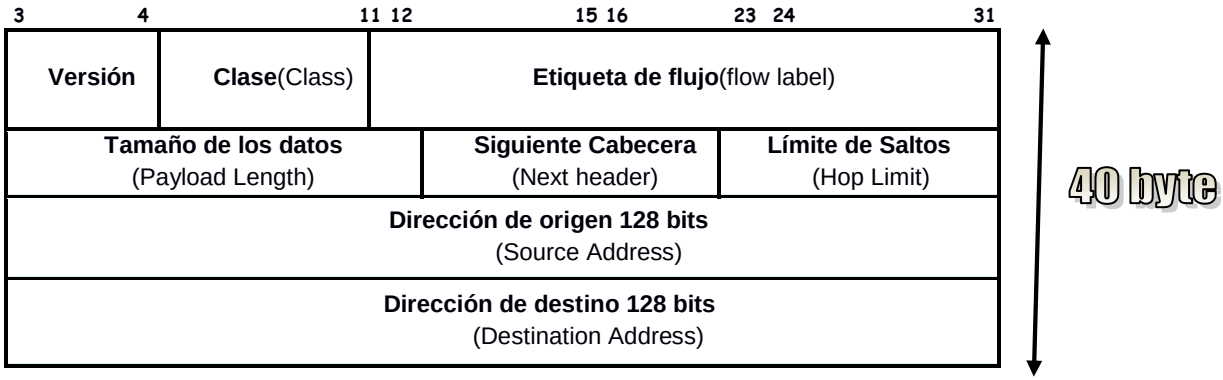



Figura 1.2 Datagrama IPv6 [2]

### 1.2.1 Forma general de un datagrama IPv6

[2] La RFC 2460 especifica la forma general de la cabecera IPv6, IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos:

- Versión: (4 bits).

Número de versión del protocolo IP, que en este caso contendrá el valor 6 y permite de una forma sencilla y rápida discriminar qué versión de datagrama se recibe, facilitando a los enrutadores el proceso de discriminar entre versión 4 y versión 6.

- Prioridad o Clase (class): (8 bits)

El campo clase de trafico está disponible para ser usados por nodos originantes y/o enrutadores reenviantes para identificar y distinguir entre las diferentes clases o prioridades de paquetes IPv6.

- Etiqueta de Flujo (Flow Label): (20 bits).

Este campo en la cabecera IPv6 puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por los enrutadores IPv6, tal como la calidad de servicio no estándar o el servicio en “tiempo real”.

- Tamaño de los Datos (Payload Length): (16 bits)

Permite un tamaño máximo de 2ˆ16 = 65536 bytes (64K). No obstante, a diferencia de la versión 4, este número hace referencia solo al tamaño de los datos que transporta, sin incluir la cabecera.

- Siguiente Cabecera (Next Header): (8 bits)

Si tras el datagrama existiera alguna extensión u opción, se le indicara al enrutador. Describe con más detalle al datagrama.

- Límite de saltos: ( 8 bits )

Es el número de saltos máximo que le queda al paquete. El límite de saltos es establecido a un valor máximo por el origen y decrementado en 1 cada vez que un nodo encamina el paquete. Si el límite de saltos es decrementado y toma el valor 0, el paquete es descartado.

- Dirección origen: (128 bits)

Es la dirección del origen del paquete.

- Dirección Destino: (128 bits)

Es la dirección del destino del paquete.

Las cabeceras de extensión definidas en IPv6, se colocan en forma de cadena después de los datos (Daisy Chain o conexiones múltiples) permitiendo personalizar el datagrama de esta manera se pueda tener varias extensiones de cabecera tan solo indicando en el campo siguiente la cabecera de cada una de ellas, el tipo de la cabecera que vendrá a continuación. En la figura 1.3 se detalla las cabeceras de extensión.

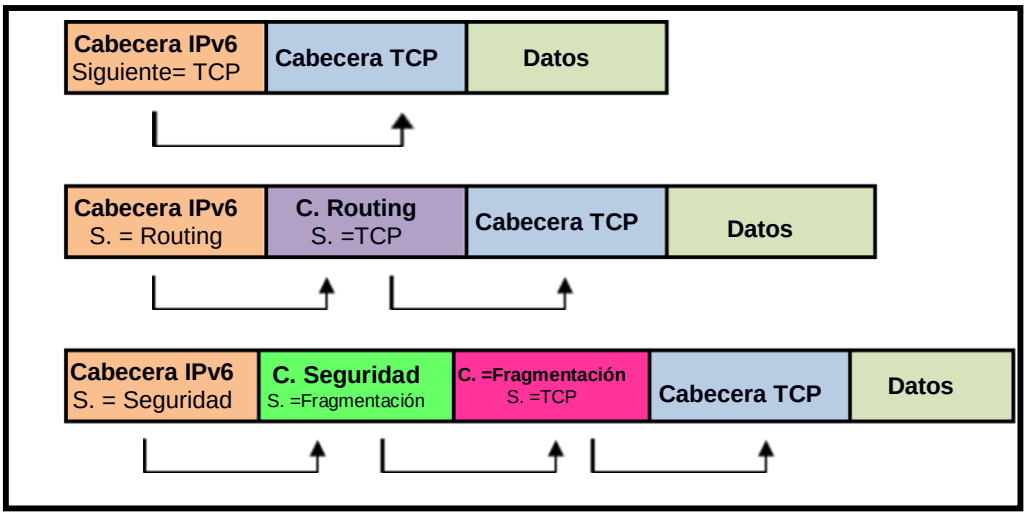



Figura 1.3 Cabeceras de Extensión [4]

## 1.3 Direccionamiento del Protocolo de Internet Versión 6.

[5] Las direcciones IPv6 están compuestas de 8 campos de 16 [bit] de largo, separados por dos puntos " : ". Cada campo está representado por 4 caracteres hexadecimales (0 - F). Un ejemplo de dirección IPv6 valida es:

**2001:0DB8:130F:0000:0000:09C0:876A:130B**

De los 128 bits, 64 bits identifican a la red y los otros 64 identifican al nodo. En la figura 1.4 se detalla la representación de una dirección IPv6.

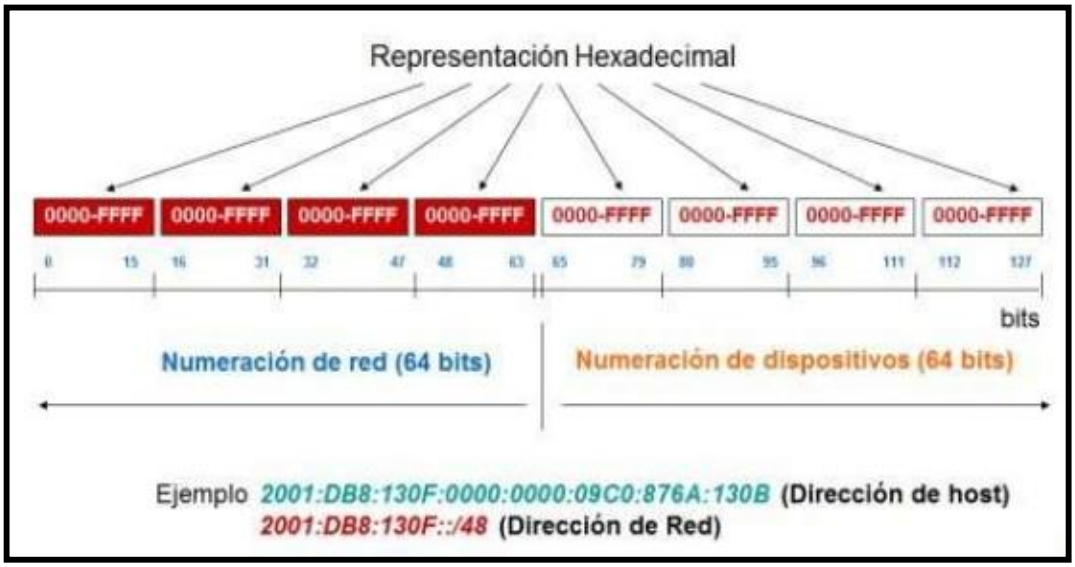



Figura 1.4 Dirección IPv6 [6]

[9] En IPv6 se han definido 3 tipos de direcciones:

- “Unicast”: Identifican a un nodo único y particular.

- “Multicast”: Identifican a un grupo de nodos. El tráfico enviado a una dirección “multicast” es reenviado a todos los nodos pertenecientes al grupo.

- “Anycast”: Identifica a un grupo de nodos. El tráfico enviado a una dirección “anycast” es enviado al nodo más cercano al emisor.

Se han eliminado las direcciones del tipo “broadcast”, reemplazando su uso con direcciones “multicast” que identifican a determinados grupos de dispositivos en una red.

### 1.3.1 Envío de información hacia un único destino (Unicast)

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

Uno de los nuevos aspectos introducidos en IPv6 es el uso de contextos en las direcciones Unicast. Los contextos definen el dominio de una red, ya sea lógico o físico. El poder reconocer el contexto al que pertenece una determinada dirección permite realizar un manejo óptimo de los recursos de la red, optimizando su desempeño.

En IPv6, las direcciones unicast pueden pertenecer a uno de los tres contextos existentes:

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

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

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

Estos contextos presentan una estructura jerárquica, tal como se observa en la Figura 1.5. El contexto global es el más amplio, englobando al resto.

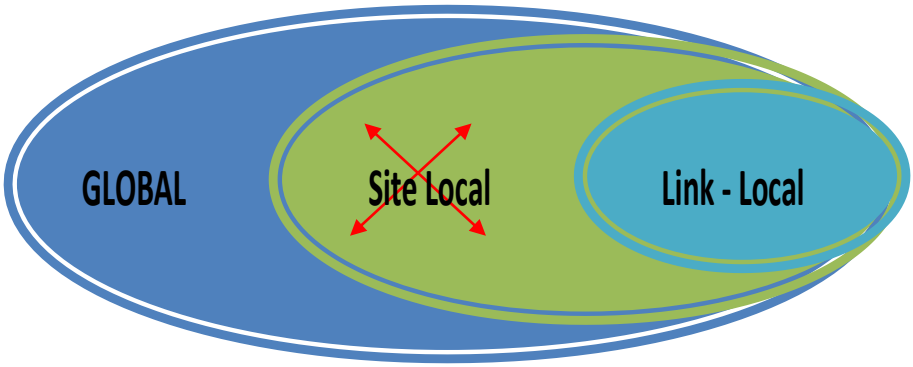



Figura 1.5 Contextos de direcciones Unicast [4]

[7] El protocolo IPv6 permitirá que la comunicación entre nodos sea de extremo a extremo y el uso de “Site-Local” implicará la utilización de direcciones privadas que dieron grandes problemas para la administración de red y desarrollo de aplicaciones, motivo por el cual fue desaprobado en la RFC 3879.

[8] El grupo de trabajo de la IPV6 dentro de la IETF en su RFC 4193 consideró una alternativa al “Site-Local” que es “Unique Local IPv6 Unicast Address”.

Una dirección local única es una dirección unicast IPv6 que es único en el mundo y que está previsto para las comunicaciones locales. Se detalla en la figura 1.6 el formato de Unique Local IPv6 Unicast Address.

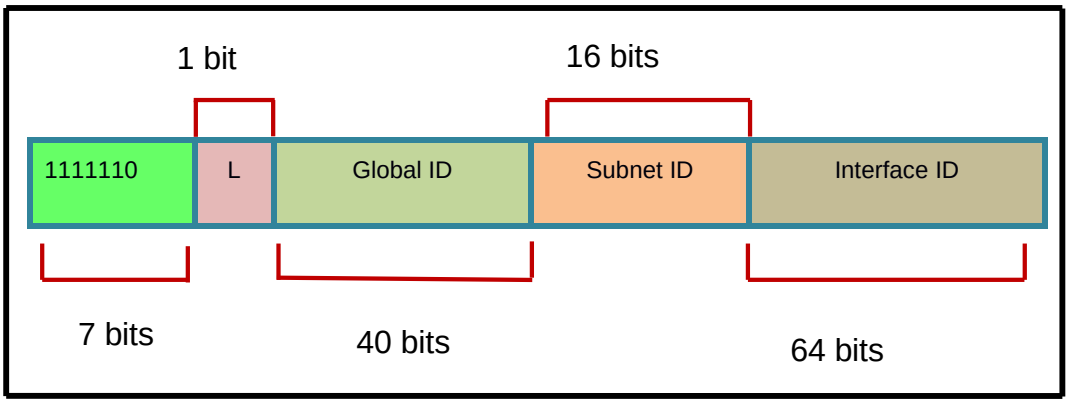



Figura 1.6 Formato Unique IPv6 Local Unicast Address [8]

L = 1 Este prefijo es asignado localmente.

L = 0 Está reservado para uso futuro.

Global ID Prefijo identificador único global

Subnet ID Prefijo identificador de Subred

Interface id Prefijo identificador de interfaz

Una dirección local única tiene las siguientes características:

- Tiene un prefijo único global (es decir, que tiene una alta probabilidad de singularidad).
- Tiene un prefijo bien conocido para permitir un sencillo filtrado en los límites del sitio.
- Es un ISP independiente y se puede utilizar para las comunicaciones dentro de un sitio sin tener cualquier conectividad a internet.
- No son enrutables a nivel mundial. Son enrutables dentro de un área más limitada, como un sitio. También pueden ser enrutadas entre un conjunto limitado de sitios.
- Si se filtró accidentalmente fuera de un sitio a través de enrutamiento o DNS, no hay conflicto con cualquier otra dirección.

A diferencia de IPv4, en IPv6 una interfaz puede poseer más de una dirección IP. Es así como por ejemplo un nodo puede poseer una dirección local al enlace para comunicarse con los dispositivos locales y una o más direcciones globales para comunicarse hacia Internet.

DIRECCIONES UNICAST LOCALES AL ENLACE.

[34] Las direcciones Unicast locales al enlace son aquellas que permiten la comunicación entre los distintos nodos conectados a un mismo enlace capa 2 del modelo ISO/OSI. Estas direcciones no pueden ser enrutadas y solo son válidas al interior del enlace.

Cada vez que un nodo IPv6 se conecta a una red, adquiere automáticamente una dirección local al enlace, sin ser necesaria la intervención del usuario o de otros dispositivos.

La estructura de una dirección local al enlace es “FE80:0:0:0:<identificador de interfaz>”. El identificador de interfaz se genera automáticamente a partir de su dirección MAC, siguiendo el formato EUI-64.

A continuación se detalla cómo se construye el identificador de interfaz IPv6 a partir de la dirección MAC.

Las direcciones locales al enlace permiten proveer de forma rápida y simple conectividad entre los nodos conectados a un mismo enlace. Su

principal ventaja es que no dependen de los prefijos IPv6 anunciados en una red, por lo que permiten identificar directamente a los nodos y enrutadores presentes en un enlace.

- Identificador de Interfaz: Individualiza a una interfaz presente en una determinada subred del sitio. A diferencia de las direcciones locales al enlace, este identificador no se genera automáticamente. La figura 1.7 me muestra cómo se obtiene el identificador de Interfaz.

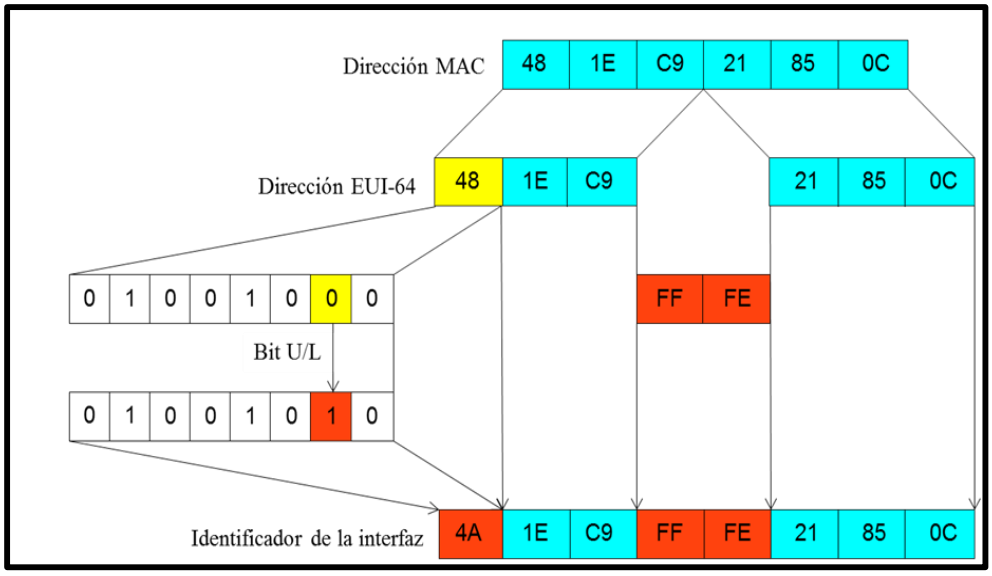



Figura 1.7 Creación del identificador de interfaz [4]

DIRECCIONES UNICAST GLOBALES

[11] Las direcciones unicast globales son usadas para comunicar 2 nodos a través de Internet. Son el equivalente a las direcciones públicas en IPv4. Son el único tipo de direcciones que pueden ser encaminadas a través de Internet.

Todas las subredes en el espacio de direccionamiento unicast global tienen un prefijo de red fijo e igual a /64. Esto implica que los primeros 64[bit] (los primeros 4 campos en formato hexadecimal) corresponden al identificador de red, y los siguientes corresponden a la identificación de la interfaz de un determinado nodo. En su forma general las direcciones unicast globales están definidas como se muestra en la figura 1.8.

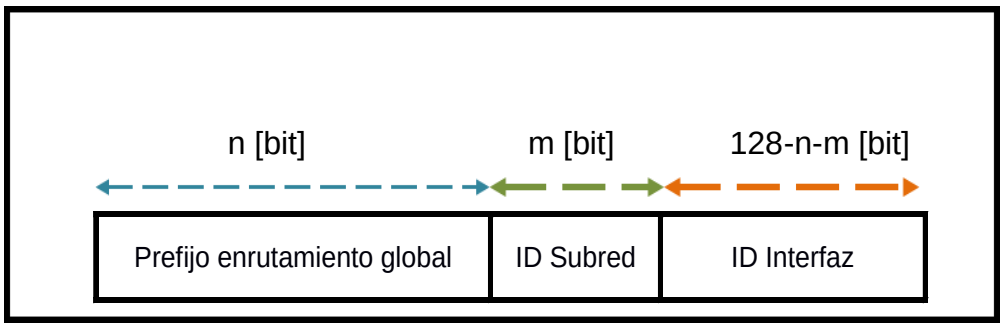



Figura 1.8 Estructura de una dirección unicast global [11]

El prefijo de enrutamiento global es aquel que identifica a un sitio conectado a Internet. Dicho prefijo sigue una estructura jerárquica, con el fin de reducir el tamaño de la tabla de enrutamiento global de Internet. En la figura 1.9 se presenta la estructura utilizada actualmente para la delegación de prefijos.

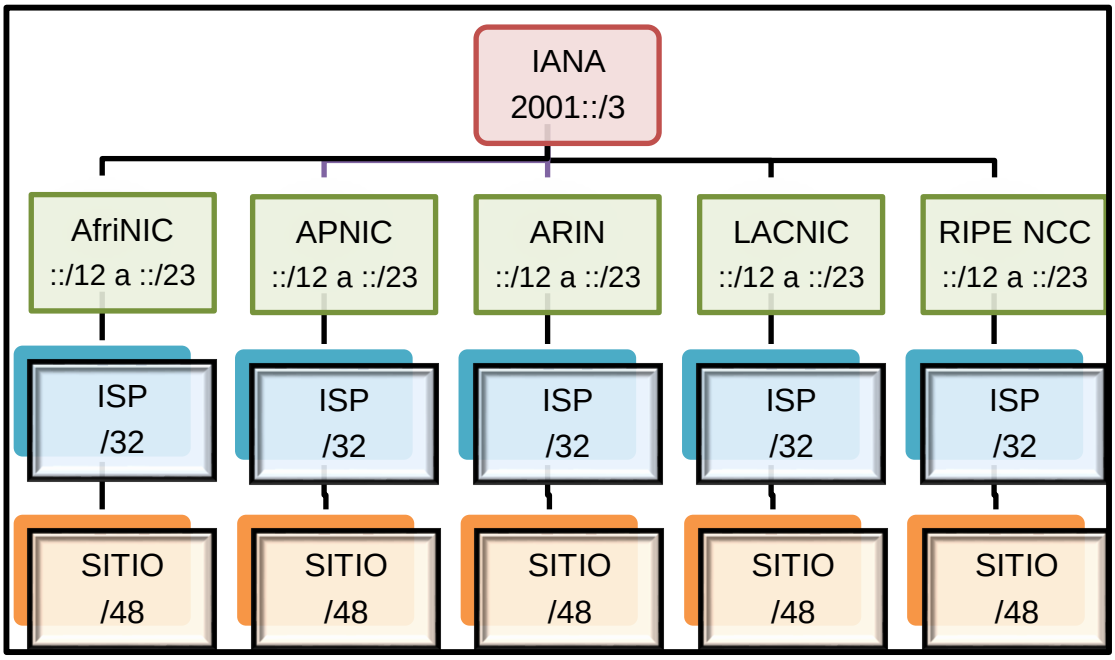



Figura 1.9 Jerarquía de delegación de prefijos unicast globales [9]

### 1.3.2 Envío de información hacia varios destinos (Multicast)

[9] En IPv6 el tráfico Multicast opera de la misma forma que en IPv4. Dispositivos IPv6 ubicados en distintos lugares pueden recibir tráfico dirigido a una única dirección Multicast. La estructura de una dirección multicast es detallada en la figura 1.10.

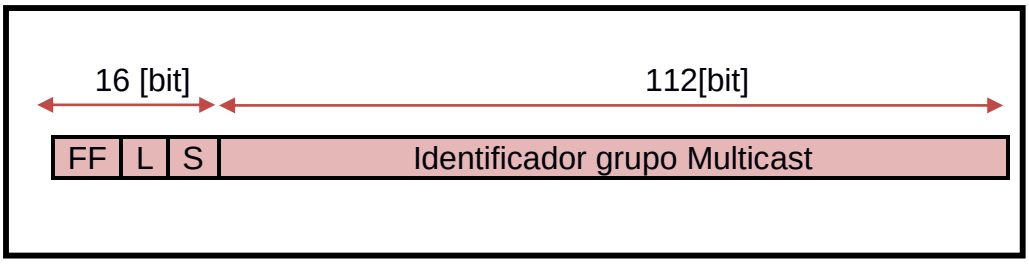



Figura 1.10 Estructura direcciones multicast [9]

El campo L indica el tiempo de vida de un grupo Multicast, tomando el valor de 0 cuando es un grupo permanente y 1 cuando es un grupo Multicast temporal. El campo S indica el contexto o alcance del grupo, de acuerdo a los valores presentados en la Tabla 1.1.

Tabla 1.1 Códigos de contexto en una dirección multicast [9]

| Valor de S(hexadecimal de 4 [bit] | Contexto del grupo |
|---|---|
| **1** | Interfaz |
| **2** | Enlace |
| **5** | Sitio |
| **8** | Organización |
| **E** | Global |
| **Otros valores** | Sin asignar o reservado |

La figura 1.11 muestra cómo se produce la comunicación unicast, es decir hacia un único destino.

Diferencia entre Unicast y Multicast.

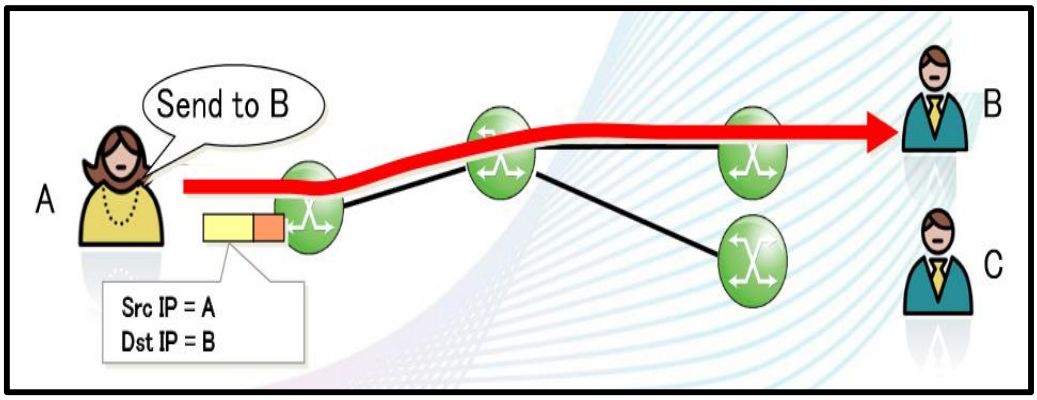



Figura 1.11 Comunicación Unicast [10]

La comunicación multicast como se detalla en la figura 1.12 permite la comunicación de uno a un grupo de usuarios.

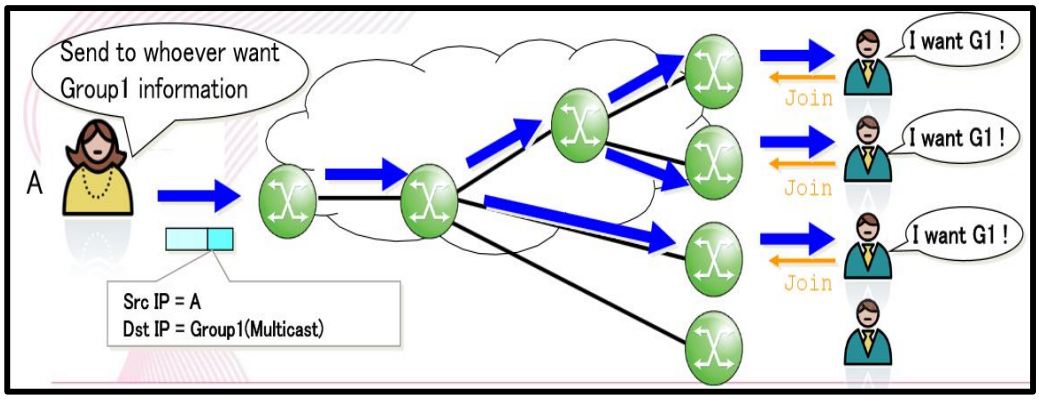



Figura 1.12 Comunicación Multicast [10]

### 1.3.3 Envío de información hacia el mejor destino (Anycast)

[5] Una dirección IPv6 anycast es una dirección que se asigna a más de una interfaz(típicamente pertenecientes a diferentes nodos), con la propiedad de que un paquete enviado a una dirección anycast se dirige a la interfaz más cercana que tenga esa dirección, de acuerdo con la métrica de enrutamiento.

Las direcciones Anycast se asignan a partir del espacio de direcciones unicast, usando cualquiera de los formatos definidos en las direcciones unicast.

El uso de anycast permite entre otras cosas implementar balanceo de carga y tolerancia a fallas. Por lo general, su uso se suele restringir al contexto de un sitio o red local. Las direcciones anycast, al igual que las multicast solo son válidas como direcciones de destino en los paquetes IPv6.

## 1.4 Algoritmos de Enrutamiento del Protocolo de Internet Versión 6

[12] El uso de IPv6 no implica cambios significativos en la forma en que operan los protocolos de enrutamiento en las redes IP. Sin embargo, para aprovechar las nuevas características de IPv6, se han desarrollado nuevas versiones o complementos a los protocolos de enrutamiento más utilizados. La tabla 1.2 muestra los protocolos de enrutamiento IPv4 y su equivalente en la versión IPv6.

Tabla 1.2 Protocolos de enrutamiento en IPv6 [12]

| Protocolo Enrutamiento IPv4 | Protocolo Enrutamiento Versión IPv6 |
|---|---|
| **RIP** | RIPng |
| **EIGRP** | EIGRP para IPv6 |
| **OSPF** | OSPFv3 |
| **IS-IS** | Integrated IS-IS |
| **BGP** | BGP-MP |

### 1.4.1 Protocolo de Mensajes de Control de Internet Versión 6 (ICMPv6)

[13] El protocolo de mensajes de control de Internet (ICMP) es utilizado para enviar información de configuración y reportes de error entre los nodos de una red. Para IPv6, se ha desarrollado una versión del protocolo, denominado ICMPv6.

A diferencia de ICMP para IPv4, el cual no es esencial para las comunicaciones en redes IPv4, ICMPv6 posee características imprescindibles para la configuración y comunicación en redes IPv6. El protocolo ICMPv6 comprende una serie de mensajes, cada uno identificado con un código. Dichos mensajes permiten llevar a cabo diversos procesos en IPv6 tales como: descubrimiento del máximo valor MTU en un camino, manejo de grupos multicast, detección de destinos inalcanzables y el protocolo de descubrimiento de vecinos.

### 1.4.2 Protocolo de descubrimiento de vecinos (Neighbor Discovery)

[14] El protocolo de descubrimiento de vecinos (Neighbor Discovery Protocol, NDP) es un protocolo necesario para el correcto funcionamiento de las redes IPv6. Es el encargado de descubrir otros nodos en el enlace, realizar la resolución de direcciones IPv6 y direcciones MAC, encontrar los enrutadores disponibles y mantener información actualizada sobre el estado de los caminos hacia otros nodos.

Este protocolo realiza funciones para IPv6 similares a las realizadas por ARP en IPv4. Para el intercambio de información, utiliza mensajes ICMPv6. La tabla 1.3 muestra las características del protocolo de descubrimientos de vecinos.

Tabla 1.3 Características protocolo descubrimiento de Vecinos. [9] [14]

| Característica de NDP | Descripción | Equivalente IPv4 |
|---|---|---|
| Descubrimiento de enrutadores | Permite a los dispositivos detectar a los enrutadores presentes en el enlace. | ICMP *Router* Discovery |
| Descubrimiento de Prefijo | Permite a los nodos conocer el prefijo utilizado en el enlace. | No disponible |
| Descubrimiento de Parámetros | Permite a los nodos auto-configurar parámetros como MTU o número máximo de saltos. | PMTU Discovery |
| Configuración Automática de direcciones | Permite a los dispositivos auto configurar su propia dirección | No disponible |
| Resolución de direcciones | Permite a los nodos determinar las direcciones capa 2 de los dispositivos presentes en el enlace | ARP |
| Determinación próximo salto | Permite a los nodos determinar el próximo salto para un destino dado. | Tabla ARP y/o tabla de enrutamiento en los dispositivos. |
| Detección de vecinos inalcanzables (NUD) | Detecta si se puede alcanzar un determinado nodo. | "Dead Gateway Detection" |
| Detección de direcciones duplicadas (DAD) | Permite a los nodos determinar si una dirección está en uso. | ARP con origen=0 |
| Redirección | Permite a los *encaminadores* informar a los nodos de un mejor próximo salto para una dirección en particular | ICMPv4 Redirect |

## 1.5 Configuración automática en Protocolo de Internet Versión 6

### 1.5.1 Introducción

[15] IPv6 nos permite configurar de tres maneras distintas una dirección IPv6 en un hosts: de forma estática, mediante configuración automática sin intervención (Stateless) o mediante DHCPv6 (Stateful).

La Configuración Automática “Stateless” (sin intervención), no requiere ninguna configuración manual del hosts, configuración mínima (o ninguna) de enrutadores, y no precisa servidores adicionales.

Permite a un hosts generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los enrutadores. Los enrutadores anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras el hosts genera un “identificador de interfaz”, que identifica de forma única la interfaz en la subred. La dirección se compone por la combinación de ambos campos. En ausencia del enrutador, el *terminal* solo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al

mismo enlace. La configuración automática nos permite afirmar que IPv6 es “Plug & Play”.

En la configuración automática “Stateful” (predeterminada), el hosts obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada hosts.

### 1.5.2 Configuración automática de Direcciones de Protocolo de Internet versión 6 “sin intervención” (Stateless).

[15] El procedimiento para la configuración automáticamente sin intervención utiliza el protocolo de descubrimiento de vecinos NDP para reconocer los enrutadores que están presentes en el enlace y generar una dirección IPv6.

Cuando se inicia la configuración automática los nodos escuchan los mensajes RA que envían los enrutadores o pueden enviar un mensaje de solicitación de enrutadores RS. A partir de los mensajes RA, se obtiene la información del prefijo de red.

Para generar la dirección IPv6 el hosts genera un identificar de interfaz. Ya sea de forma aleatoria o mediante el uso de la dirección MAC ADDRES. Luego sigue un proceso de verificación antes de ser utilizada la dirección IPv6.

1. Verificar que dicha dirección “tentativa” puede ser asignada (no está duplicada en el mismo enlace).

2. Si esta duplicada, la Configuración Automática se detiene, y se requiere un procedimiento manual (por ejemplo, usando otro identificador de interfaz).

3. Si no está duplicada, la conectividad a nivel IP se ha logrado, al asignarse definitivamente dicha dirección “tentativa” a la interfaz en cuestión.

4. Si se trata de un terminal, se interroga a los posibles enrutadores para indicar al terminal lo que debe de hacer a continuación.

5. Si no hay enrutadores, se invoca el procedimiento de Configuración Automática “stateful”.

6. Si hay enrutadores, estos contestaran indicando fundamentalmente, como obtener las direcciones si se ha de utilizar el mecanismo “stateful”, u otra información, como tiempos de vida, etc.

### 1.5.3 Configuración automática de Direcciones de Protocolo de Internet versión 6 “Predeterminada” (Stateful).

[15] DHCP para IPv6 es un protocolo UDP cliente /servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisan un control sobre la asignación de los recursos de la red, superior al facilitados por el mecanismo de configuración “stateless”.

Los objetivos de DHCPv6 son:

- DHCP es un mecanismo, no una política. La política es establecida por el administrador de la red y DHCP le permite propagar los parámetros adecuados, según dicha política.

- DHCP es compatible, lógicamente, con el mecanismo de Configuración Automática “stateless”.

- DHCP no requiere configuración manual de parámetros de red en clientes DHCP, excepto en casos donde dicha configuración se requiere debido a medidas de seguridad.

- DHCP no requiere un servidor en cada enlace, dado que debe funcionar a través de relés DHCP.

- DHCP coexiste con nodos configurados estáticamente, así como con implementaciones existentes en la red.

- Los clientes DHCP pueden operar en enlaces donde no hay enrutadores IPv6.

- Los clientes DHCP proporcionan la habilidad de renumerar la red.

- Un cliente DHCP pueden hacer múltiples y diferentes peticiones de parámetros de configuración, de uno o varios servidores DHCP simultáneamente. DHCP proporciona suficiente información para permitir a los servidores DHCP el seguimiento del estado de configuración de los clientes.

- DHCP incorpora los mecanismos apropiados de control de tiempo y retransmisiones para operar eficazmente en entornos con una alta latencia y/o reducido ancho de banda.

## 1.6 Seguridad en Redes con Protocolo de Internet Versión 6 (IPv6).

### 1.6.1 Introducción en el Protocolo de Seguridad de Internet IPSec.

[16] 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 terminales, 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 enrutador o un Cortafuegos implementando IPSec es un Security Gateway.

Cuando se implementa IPSec en un enrutador, este provee una fuerte seguridad que puede ser aplicada a todo el tráfico que cruza por el enrutador. 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 enrutador o al cortafuego.

También IPSec es transparente a los usuarios finales. Como una política general, puede asumirse que no es necesario involucrar a los usuarios en los mecanismos de seguridad.

Los beneficios de IPv6 importantes son:

- Herencia de niveles de seguridad, de enrutadores a subredes.
- Transparencia respecto a las aplicaciones.
- Transparencia respecto a usuarios finales.
- Ofrecimiento de seguridad a nivel individual.

### 1.6.1.1 Características Generales

[17] IPSec autentifica los equipos y cifra los datos para su transmisión entre hosts en una red, intranet o extranet, incluidas las comunicaciones entre terminales 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.

La arquitectura IPsec se puede resumir en la figura 1.13.

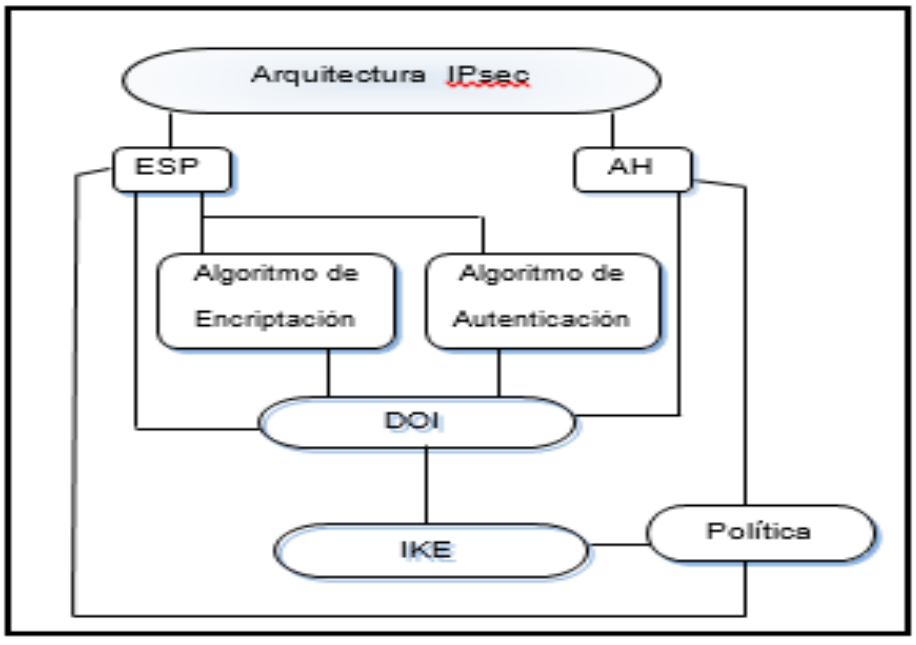



Figura 1.13 Arquitectura IPSec [17]

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

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.

### 1.6.1.2 Asociaciones de Seguridad

[16] Una Asociación de Seguridad (SA) es una conexión lógica unidireccional simplex que ofrece servicios de seguridad al tráfico transportado por este.

Está definida para comunicaciones en un solo sentido (simplex) esto significa que cada par de sistemas que se comunican por lo menos tiene dos SAs, una de origen a destino y otra de destino a origen.

Lo mismo ocurre para la asociación de seguridad que se crea para AH o ESP, si estos dos protocolos se aplican a una comunicación juntos, se crearan dos o más asociaciones de seguridad.

Para la identificación de una asociación de seguridad se utiliza un índice de parámetros de Seguridad (Security Parameter Index, SPI) el cual contiene la dirección destino y el identificador de protocolo de seguridad (AH y ESP); con esta información el índice de Parámetros de Seguridad puede recibir un datagrama y saber a qué

asociación de seguridad hace referencia, y de esta forma poder autentificarlo y/o descifrarlo.

Una asociación de seguridad describe:

- Que algoritmo va a ser usado en la autenticación y las claves para él.
- El algoritmo de cifrado y las claves.
- Tiempo de vida de las claves.
- Tiempo de vida de la SA
- Dirección IP origen de la SA

1.6.1.3 Autentificación

[18] La Autentificación se refiere al servicio mediante el cual se garantiza que una de las partes llamada el solicitante, que tiene la identidad de principal, solicita la autenticación de esta y permite a otra parte llamada el verificador declarar que la solicitud es legítima.

El servicio de autentificación se basa en alguno de los siguientes métodos:

- El solicitante demuestra el conocimiento de algo, por ejemplo: una clave.
- El solicitante demuestra poseer algo, por ejemplo: una tarjeta inteligente, dispositivo USB tipo token.
- El solicitante presenta una característica inmutable, por ejemplo: una huella digital, verificación de voz o patrones oculares.
- Una evidencia de que el solicitante está en un lugar determinado en un momento determinado
- El verificador acepta la autentificación realizada por terceros.

#### 1.6.1.4 Encriptación.

[18] Con la encriptación podemos transformar un texto plano a texto cifrado, con la posibilidad de recuperar luego el texto plano a partir del texto cifrado.

Este proceso de transformación/recuperación se lleva a cabo siguiendo un procedimiento preestablecido conocido como algoritmo de encriptación, que depende principal de un parámetro denominado clave o clave secreta. La figura 1.14 describe el proceso de encriptación.

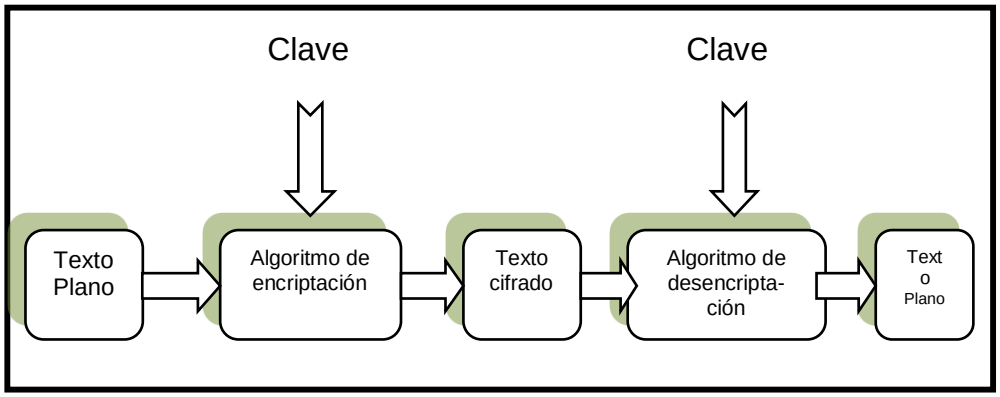



Figura 1.14 Proceso de Encriptación [18]

Existen dos métodos de encriptación que son los más usados son: encriptación simétrica y encriptación asimétrica.

**Encriptación simétrica.**

[18] Es aquella donde la misma clave –que debe mantenerse en secreto- sirve para encriptar y desencriptar la información. Llamada encriptación clásica, convencional o de una sola clave, se usa básicamente al requerir una performance rápida de encriptación. Para fortalecer la seguridad la clave de sesión debe cambiarse con la mayor frecuencia posible. El proceso de Encriptación Simétrica es detallado en la figura 1.15.

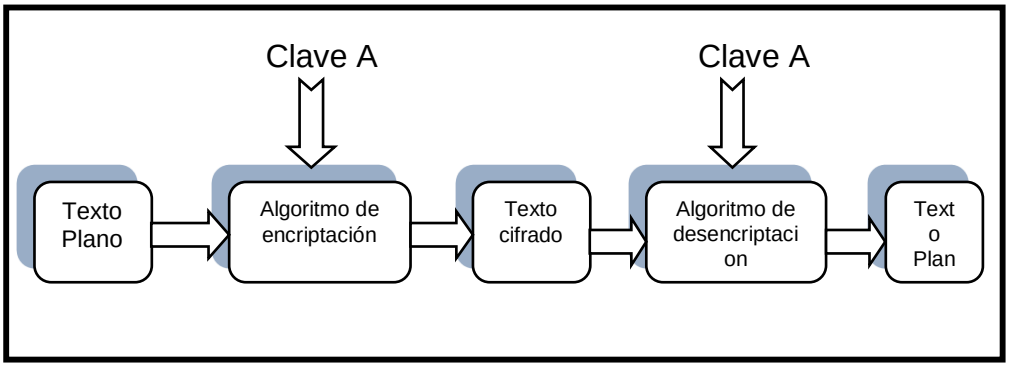



Figura 1.15 Proceso de Encriptación Simétrica [18]

Aunque la encriptación simétrica solo utiliza una clave compartida, debemos tener en consideración los siguientes detalles antes de implementar este tipo de encriptación.

- Las claves deben permanecer secretas.
- Las claves deben cambiarse periódicamente.
- En grandes ambientes, generar, distribuir y proteger las claves resulta una labor compleja.

Un método común de encriptación simétrica es el que se realiza por medio de la Norma de Encriptación de Datos (Data Encryption Standard-DES).

**Encriptación Asimétrica.**

Este método también es conocido como encriptación de clave pública, debido a que es el esquema de encriptación usa dos claves: una privada y una pública.

**Claves publicas según DIFFIE-HELLMAN**

[18] Estas claves se originan mediante el esquema de claves Diffie-Hellman, donde la clave pública de un servidor y la clave privada de otro servidor crean una clave secreta compartida, siendo matemáticamente casi imposible derivar la clave privada a partir de la clave pública. Esta clave secreta compartida se utiliza para verificar y desencriptar el paquete cifrado.

El procedimiento para realizar una encriptación asimétrica es el siguiente:

- El servidor A envía su clave pública al servidor B, el cual también comparte su clave pública.

- La clave privada se combina con la clave pública del otro servidor, utilizando el algoritmo Diffie-Hellman para generar la clave secreta compartida.

- La encriptación es segura porque nadie, excepto los servidores A y B, puede reproducir la clave secreta compartida. El proceso de Encriptación Asimétrica se muestra en la figura 1.16.

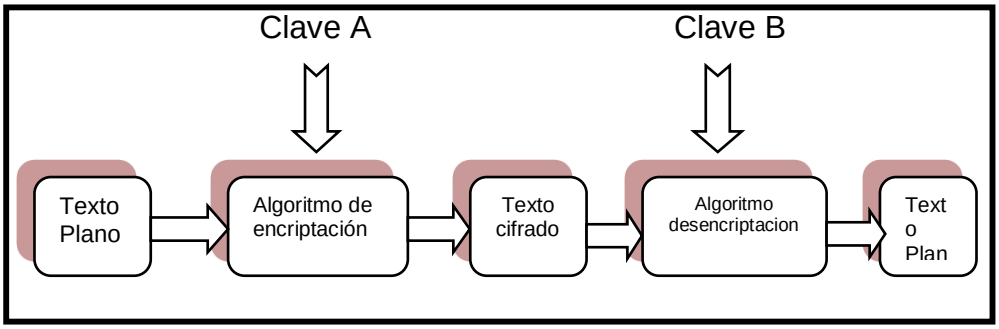



Figura 1.16 Proceso de Encriptación Asimétrica [18]

La tabla 1.4 muestra los algoritmos de Encriptación.

Tabla 1.4 Algoritmos de Encriptación [18]

| | NORMA | TIPO | TAMAÑO DE CLAVE | EXPLICACION |
|---|---|---|---|---|
| 1 | 3DES (TDES) | Privada | 40, 56 bits | Triple DES usa dos o tres claves y pases múltiples. |
| 2 | DES | Privada | 40, 56 bits | Normas de encriptación digital ampliamente usada para la encriptación de claves privadas. |
| 3 | DSA | Firma Digital | 1024 bits | Un algoritmo de firma digital genera firmas digitales anexadas a los documentos originales para garantizar que no hayan sido alterados. |
| 4 | ECC | Publica | 160 bits | *Elliptical Curve Cryptography*. Produce una seguridad equivalente a la clave RSA de 1024 bits con solo 160 bits. |
| 5 | IDEA | Privada | 128 bits | Algoritmo de encriptación internacional de datos. Genera claves para uso en una sola sesión. Se usa en PGP (Pretty Good Privacy) |
| 6 | MD5 | Digest | | Produce números Hash de 128 bits, basados en documentos originales. Pueden incorporarse dentro de las firmas digitales. Reemplaza al MD4 y al MD5. |
| 7 | RCA | Publica | 512 a 2048 bits | Norma popular de encriptación pública. La longitud de clave recomendada es 1024 bits. |
| 8 | Skipjack | Privada | 80 bits | Usada por los circuitos integrados de encriptación (chips) Clipper y Capstone y el Defense Messaging System. |

### 1.6.2 Protocolos de Seguridad de Internet IPSec.

#### 1.6.2.1 Protocolo AH

[19] El protocolo AH es el procedimiento previsto dentro de IPSec para garantizar la integridad y autenticación de los datagramas IP. Le 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. La figura 1.17 muestra la estructura del datagrama AH.

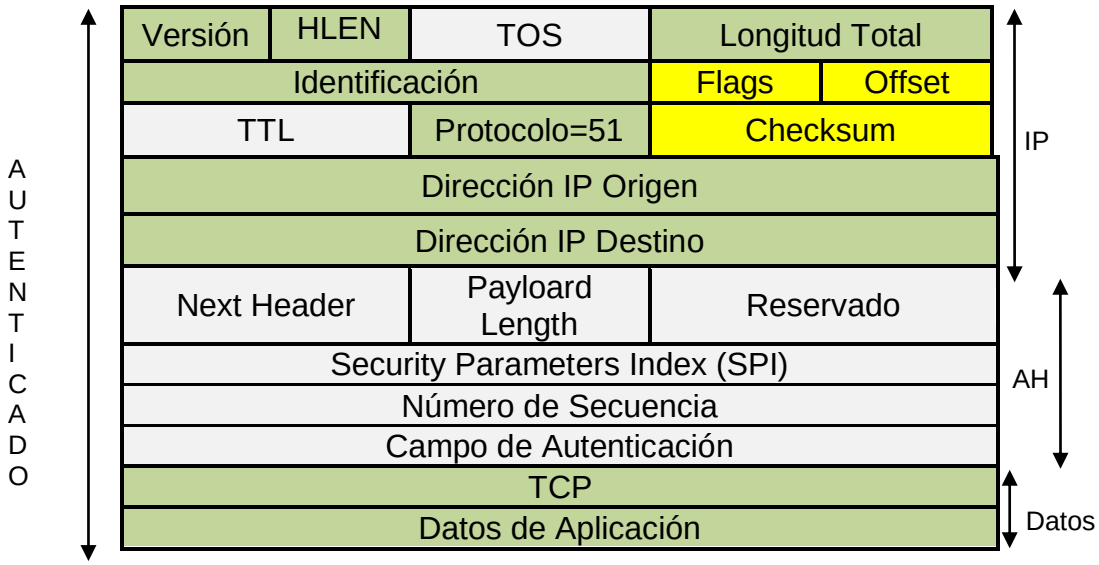



Figura 1.17 Estructura de un datagrama AH. [19]

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.

Es dentro de la cabecera AH donde se indica la naturaleza de los datos de la capa superior. Es importante destacar que AH asegura la integridad y autenticidad de los datos transportados y de la cabecera IP, excepto los campos variables: TOS, TTL, flags, offset y checksum.

El funcionamiento de AH se basa en un algoritmo HMAC, esto es, un código de autenticación de mensajes. Este algoritmo consiste en aplicar una función hash a la combinación de unos datos de entrada y una clave, siendo la salida una pequeña cadena de caracteres que denominados 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.

El emisor calcula un extracto del mensaje original, el cual se envía a través de la red, repitiéndose en el extremo receptor el

cálculo del extracto y comparándolo con el recibido en el paquete. La figura 1.18 detalla cómo funciona el protocolo AH.

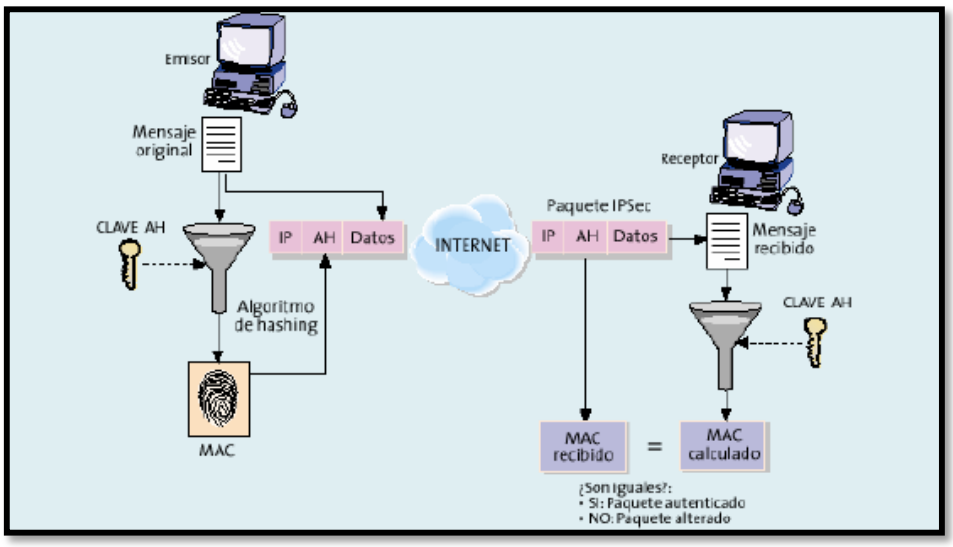



Figura 1.18 Funcionamiento del Protocolo AH [19]

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

Si analizamos con detalle el protocolo AH, podemos concluir que su seguridad reside en que el cálculo del extracto (MAC) es imposible sin conocer la clave y que dicha clave únicamente la conocen el emisor y el receptor.

### 1.6.2.2 PROTOCOLO ESP

[19] 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 como 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 (TCP, UDP o ICMP o incluso un paquete IP completo). La figura 1.19 describe la estructura del datagrama ESP.

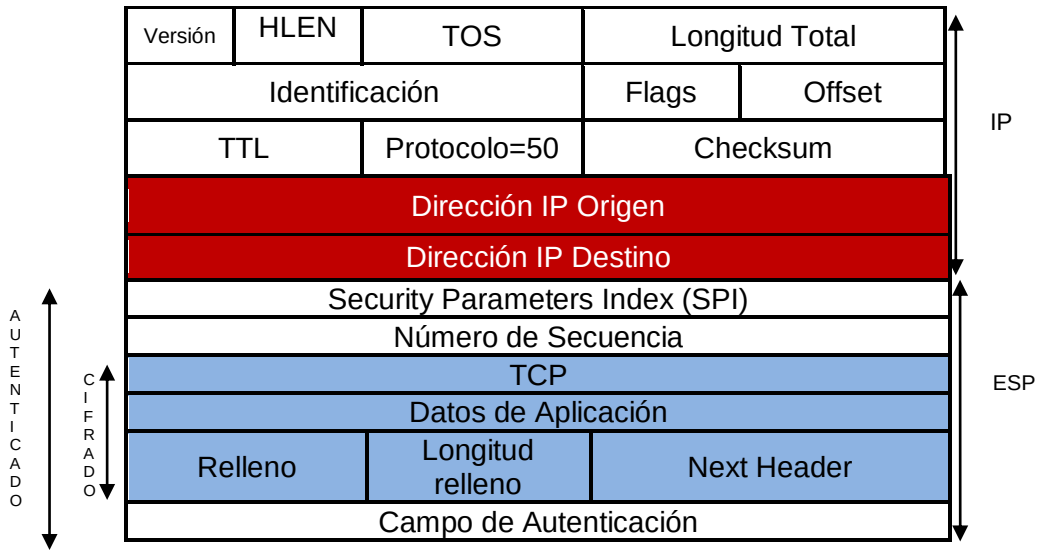



Figura 1.19 Estructura de un datagrama ESP [19]

El IANA ha asignado al protocolo ESP el número decimal 50. Esto implica que el campo protocolo de la cabecera IP contendrá el valor 50, mientras que dentro del mensaje ESP se indica la naturaleza de los datos. Puesto que este campo, al igual que la carga útil, está cifrado, un hipotético atacante que intercepte el paquete no podrá saber si el contenido es TCP o UDP; esto es completamente normal ya que el objetivo que se persigue 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 bytes). Por esta razón existe un campo de relleno, el cual tiene una función adicional: es posible añadir caracteres de relleno al campo de datos para ocultar así su longitud real y por tanto las características del tráfico.

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 transito hasta su destino, si el paquete es interceptado por un tercero solo obtendrá un conjunto de bits ininteligibles. En el destino, el receptor aplica de nuevo el algoritmo de cifrado con la misma clave, recuperando los datos originales. Este proceso es detallado en la figura 1.20.

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 como en que la clave ESP únicamente la conocen el emisor y el receptor.

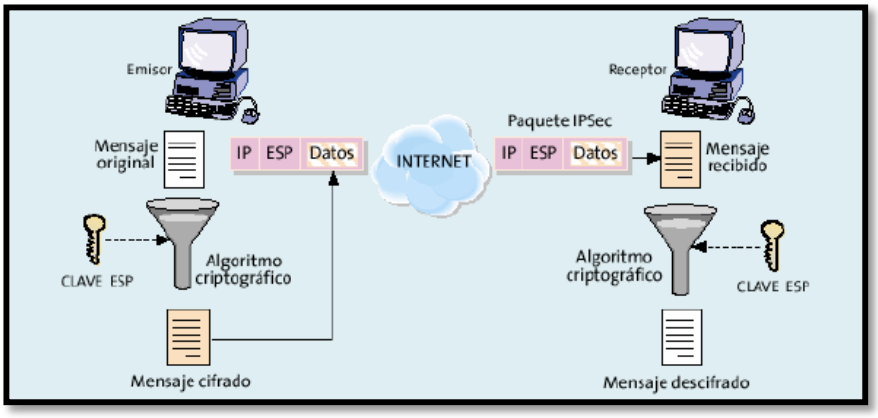



Figura 1.20 Funcionamiento del protocolo ESP [19]

La distribución de claves de forma segura es, por consiguiente, un requisito esencial para el funcionamiento de ESP y también de AH.

Es fundamental que el emisor y el receptor estén de acuerdo tanto en el algoritmo de cifrado o de hash como en el resto de parámetros comunes que utilizan.

### 1.6.2.3 PROTOCOLO IKE

[19] 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 SA´s, una por cada sentido de la comunicación.

Hasta el momento se ha supuesto 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 de le llama negociación de SA´s.

El IETF ha definido el protocolo IKE para realizar tanto esta función de gestión automática de claves como el establecimiento de las SA´s correspondientes.

Unas de las características importantes de IKE es que su utilidad no se limita a IPSec, sino que es un protocolo estándar de

gestión de claves que podría ser útil en otros protocolos, como, por ejemplo, OSPF o RIPv2.

IKE es un protocolo hibrido que ha resultado de la integración de dos protocolos complementarios: ISAKMP y Oakley.

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.

El objetivo principal de IKE consiste en establecer una conexión cifrada y autenticada entre dos entidades, a través de la cual se negocian los parámetros necesarios para establecer una asociación de seguridad IPSec.

El grafico 1.21 se muestra el funcionamiento del protocolo IKE.

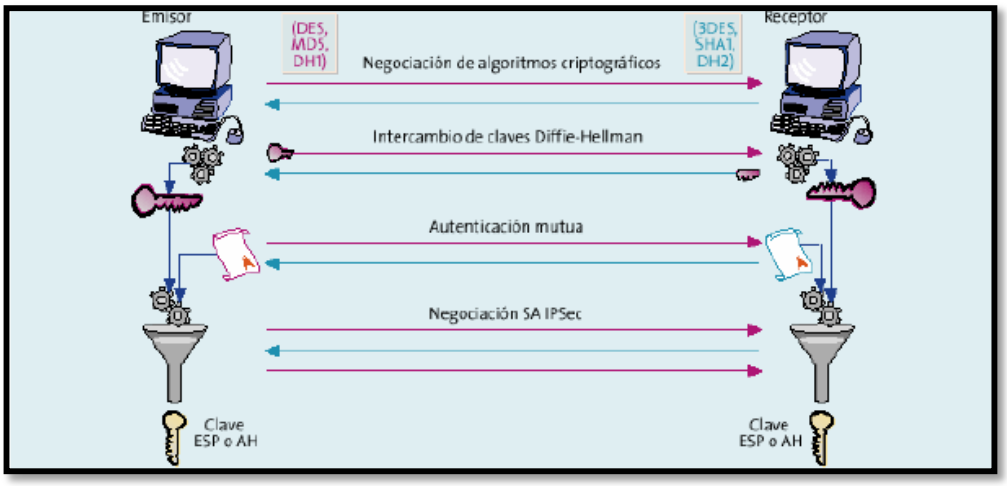



Figura 1.21 Funcionamiento del Protocolo IKE [19]

### 1.6.3 Funcionamiento del protocolo de Seguridad de Internet IPSec.

#### 1.6.3.1 Modo Transporte

[17] En modo Transporte solo 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 tiene la ventaja de que asegura la comunicación extremo a extremo, pero requiere que ambos extremos entiendan el protocolo IPSec. El funcionamiento del modo Transporte es graficado en la figura 1.22.

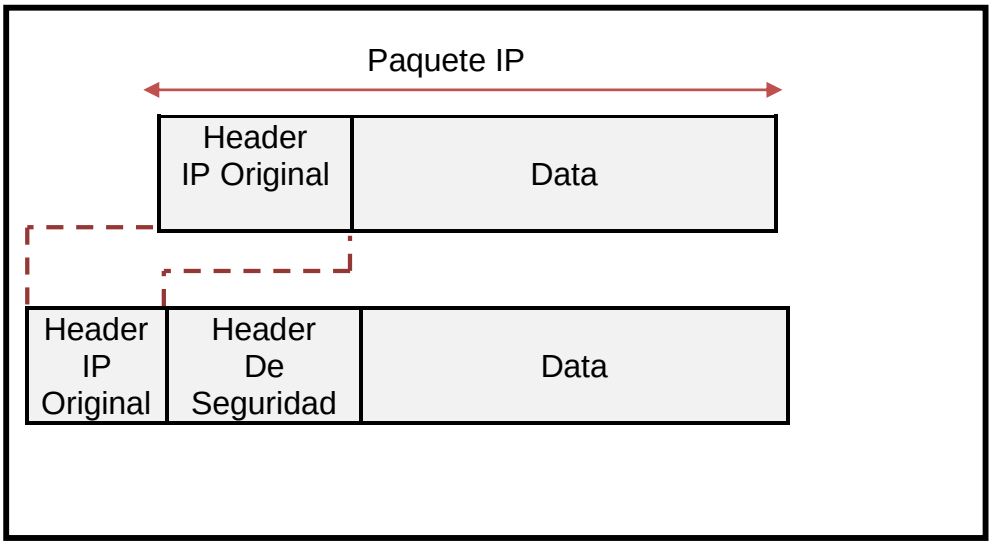



Figura 1.22 Modo Transporte IPSec [17]

1.6.3.2 Modo Túnel

[17] El contenido del datagrama AH o ESP es un datagrama IP completo, incluida la cabecera IP original. Así, se toma un datagrama al cual se añade inicialmente una cabecera AH o ESP, posteriormente se añade una nueva cabecera IP que es la que se utiliza para encaminar los paquetes a través de la red.

El modo túnel se usa normalmente cuando el destino final de los datos no coincide con el dispositivo que realiza las funciones IPSec.

IPSec puede ser implementado bien en un host o bien en un equipo dedicado, tal como un encaminador o un *cortafuegos*, que cuando realiza estas funciones se denomina *gateway(pasarela)* IPSec. En la figura 1.23 se describe la operación del modo túnel.

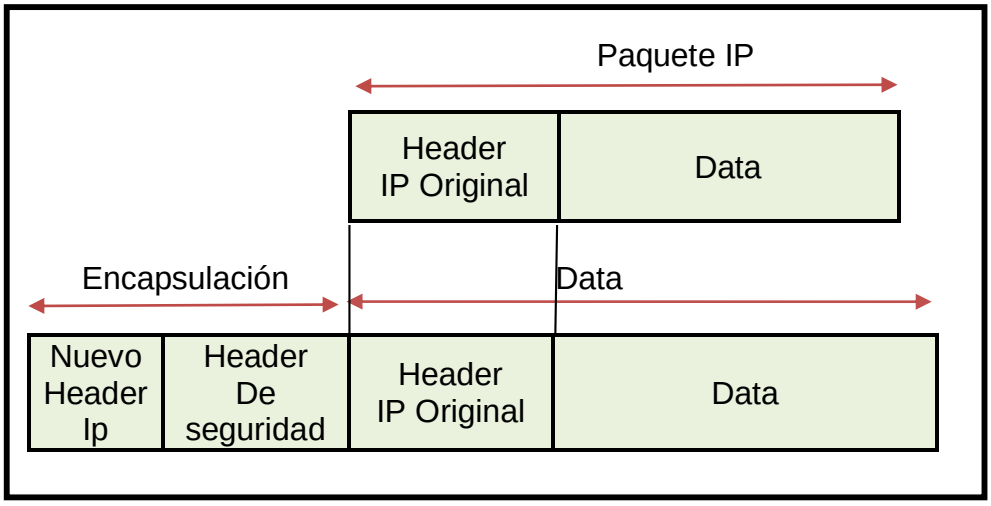



Figura 1.23 Modo Túnel IPSec [17]

### 1.6.4 Servicios de Seguridad ofrecidos por el Protocolo de Seguridad IPSec.

#### 1.6.4.1 Integridad y Autenticación del origen de los datos.

[20] El protocolo AH es el más adecuado si no se requiere cifrado. La opción de autenticación del protocolo ESP ofrece una funcionalidad similar, aunque esta protección, a diferencia de AH, no incluye la cabecera IP. Esta opción es de gran importancia para aquellas aplicaciones en las cuales es importante garantizar la invariabilidad del contenido de los datagramas IP.

#### 1.6.4.2 Confidencialidad

El servicio de confidencialidad se obtiene mediante la función de cifrado incluida en el protocolo ESP. En este caso es recomendable activar la opción de autenticación, ya que si no se garantiza la integridad de los datos, el cifrado es inútil. Esto es debido a que aunque los datos no puedan ser interpretados por nadie en tránsito, podrían ser alterados, haciendo llegar al receptor un mensaje sin sentido que sería aceptado como trafico valido.

Además de ofrecer el cifrado del tráfico, el protocolo ESP también tiene herramientas para ocultar el tipo de comunicación que se está realizando; para ello permite introducir caracteres de relleno en el contenido de los datos del datagrama, de modo que se oculta la verdadera longitud del mismo. Esta es una protección útil contra las técnicas de análisis de tráfico, que permiten a un atacante deducir información útil a partir del estudio de las características del tráfico cifrado.

#### 1.6.4.3 Control de Acceso

Dado que el uso de ESP y AH requiere el conocimiento de llaves, y dichas llaves son distribuidas de modo seguro mediante una sesión IKE en la que ambos nodos se autentifican mutuamente, existe la garantía de que solo los equipos deseados participan en la comunicación. Es conveniente aclarar que una autenticación valida no implica un acceso total a los recursos, ya que IPSec proporciona también funciones de autorización. Durante la negociación IKE se especifica el flujo de tráfico IP que circulara a través de la conexión IPSec. Esta especificación es similar a un filtro de datagramas, considerándose el protocolo, las direcciones IP de los puertos origen y destino, el byte "TOS" y otros campos.

#### 1.6.4.4 No Repudio

El servicio de no repudio es técnicamente posible en IPSec, si se usa IKE con autentificación mediante certificados digitales. En este caso, el procedimiento de autenticación se basa en la firma digital de un mensaje que contiene, entre otros datos, la identidad del participante. Dicha firma, gracias al vínculo entre la llave pública y la identidad que garantiza el certificado digital, es una prueba inequívoca de que se ha establecido una conexión IPSec con un equipo determinado, de modo que este no podrá negarlo.

# CAPÍTULO 2

## 2 PROTOCOLO SIMPLE DE ADMINISTRACIÓN DE RED (SNMP)

### 2.1 Modelo de Gestión de la Red

[21] El propósito de la gestión de redes, es la utilización y coordinación de los recursos para:

- Planificar
- Organizar
- Mantener
- Supervisar
- Evaluar y

- Controlar los elementos de las redes de comunicaciones para adaptarse a la calidad de servicio necesaria, a un determinado costo.

El monitoreo de redes es el tipo de acciones consistentes en obtener información de la red con el fin de detectar anomalías. Estas acciones son pasivas y su único objetivo es conocer el comportamiento respecto al tráfico del sistema.

### 2.1.1 Objetivos de la Gestión de Red

Los objetivos principales de la gestión de red consisten en mejorar la disponibilidad y el rendimiento de los elementos del sistema, así como incrementar su efectividad, para obtener la mejor calidad de servicio posible.

### 2.1.2 Aplicaciones

El campo de aplicación es amplio y de gran importancia dadas las características tecnológicas que poseen los sistemas de telecomunicaciones y los servicios que ofrecen. La gestión de Redes mantiene un cierto grado de complejidad al interactuar con sistemas

heterogéneos que involucran diversos fabricantes con productos eminentemente propietarios, así como productos apegados a estándares en forma total o parcial.

### 2.1.3 Clasificación de Áreas Funcionales del Gestionador de Red.

[21] Se definen las siguientes áreas funcionales para la gestión de red:

Supervisión y fallos: Conjunto de facilidades que permiten la detección, aislamiento y corrección de una operación anormal.

Configuración: Facilidades que permiten controlar, identificar, recoger y proporcionar datos a objetos gestionados, con el propósito de asistir a operar servicios de interconexión.

Contabilidad: facilidades que permiten establecer cargos por el uso de determinados objetos e identificar costes por el uso de estos.

Prestaciones: Facilidades dedicadas a evaluar el comportamiento de objetos gestionados y la efectividad de determinadas actividades.

Seguridad: Aspectos que son esenciales en la gestión de red y que permiten proteger los objetos gestionados.

### 2.1.4 Modelo Gestor – Agente

[22] Los elementos del sistema de gestión de red, bajo el esquema gestor – Agente, se clasifican en dos grandes grupos:

- Los gestores son los elementos del sistema de gestión que interaccionan con los operadores humanos y desencadenan acciones necesarias para llevar a cabo las tareas por ellos invocados.

- Los agentes, son los componentes del sistema de gestión invocados por el gestor o gestores de la red.

El intercambio de información de gestión es el principio básico, entre gestores y nodos gestionados.

## 2.2 Arquitectura del Protocolo Simpe de Administración de Red (SNMP)

SNMP es un protocolo de la capa de aplicación en el modelo OSI que facilita el intercambio de información de tipo administrativa entre los dispositivos de la red. De esta manera permite a los administradores manejar el desempeño de la red para encontrar y resolver problemas y planificar su crecimiento.

### 2.2.1 Elementos de la Arquitectura SNMP

[23] En el ambiente SNMP hay dos tipos de entidades: administrador y agente. El administrador es un servidor con algún tipo de software que puede manejar tareas administrativas para una red. En el lenguaje SNMP son referidos como Network Management Stations (NMS), es decir estaciones de administración de redes. Una estación es responsable de generar consultas y de recibir notificaciones de agentes de red. A través de una consulta se obtiene información que más tarde puede ser usada para determinar si ha ocurrido algún evento crítico.

Por otro lado una notificación permite al agente dar aviso que algo ha ocurrido.

El Agente, por su parte es una aplicación que corre en equipos de red (conmutadores, enrutadores, servidores, etc.). El agente provee información de administración a la estación no perdiendo de vista los aspectos operacionales del equipo.

Cuando el agente percibe que algo malo sucedió, él puede enviar un mensaje a la estación para volver a su estado normal. La figura 2.1 muestra la relación de trasmisión de mensajes entre el NMS y el Agente.

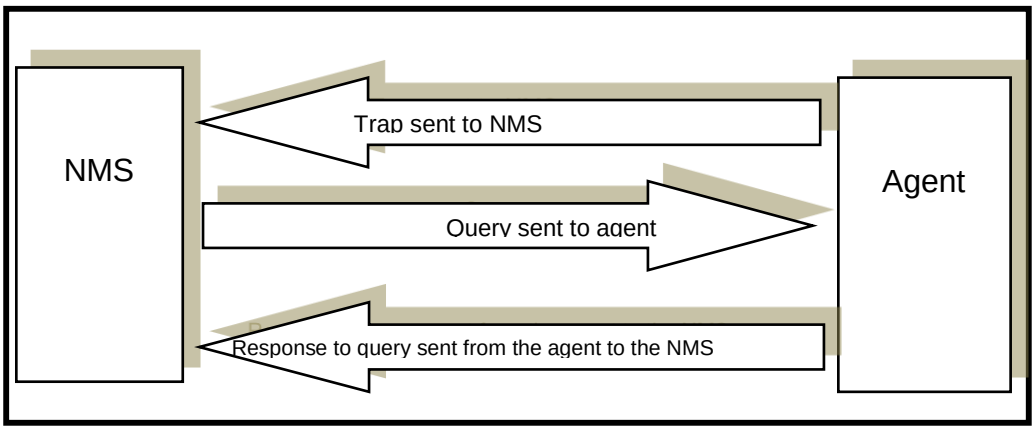



Figura 2.1 Relación entre NMS y Agente [24]

### 2.2.2 Consola de Administración NMS

[25] Una NMS es responsable de generar consultas y de recibir notificaciones de agentes en la red. A través de una consulta se obtiene información que más tarde puede ser usada para determinar si ha ocurrido algún evento crítico. La estación tiene la capacidad de realizar una acción basada en la información que recibió del agente, realizando así un monitoreo proactivo en algunos casos.

Se tiene tres arquitecturas para la administración de red: Centralizada, distribuida y jerárquica.

- **Arquitectura Centralizada**: Todas las consultas son enviadas a un sistema de gestión simple.

- **Arquitectura Distribuida**: Hay dos puntos de administración del sistema que gestiona los agentes.

- **Arquitectura Jerárquica**: Combina el sistema centralizado con el distribuido, es más complejo pero provee las fortalezas de las anteriores.

### 2.2.3 Agente

Los agentes de administración son procesos que se ejecutan en cada nodo de la red, como hosts, enrutadores, puentes, conmutadores que deben estar equipados con SNMP. Todos los datos del agente se almacenan en su MIB y entre las funciones principales que un agente puede controlar encontramos.

- Número y estado de circuitos virtuales
- Mensajes de difusión enviados y recibidos
- Numero de bytes y paquetes entrantes y salientes del dispositivo
- Interfaces de red que se han caído y las que se han activado

### 2.2.4 MIB (Management Information Base)

[21] Una MIB es un conjunto de definiciones de uno o varios recursos formado por clases de objetos gestionados, acciones, notificaciones, atributos, sintaxis, etc. Están compuestos de objetos administrados y están identificados por identificadores de objetos.

Un objeto administrado u Objeto MIB, es uno de cualquier número de características específicas de un dispositivo administrado. Los objetos administrados están compuestos de una o más instancias de objeto, que son esencialmente variables.

Un identificador de objeto (object ID) únicamente identifica un objeto administrado en la jerarquía MIB. La jerarquía MIB puede ser representada como un árbol con una raíz anónima y los niveles, que son asignados por diferentes organizaciones. Esta jerarquía del árbol MIB es graficado en la figura 2.5.

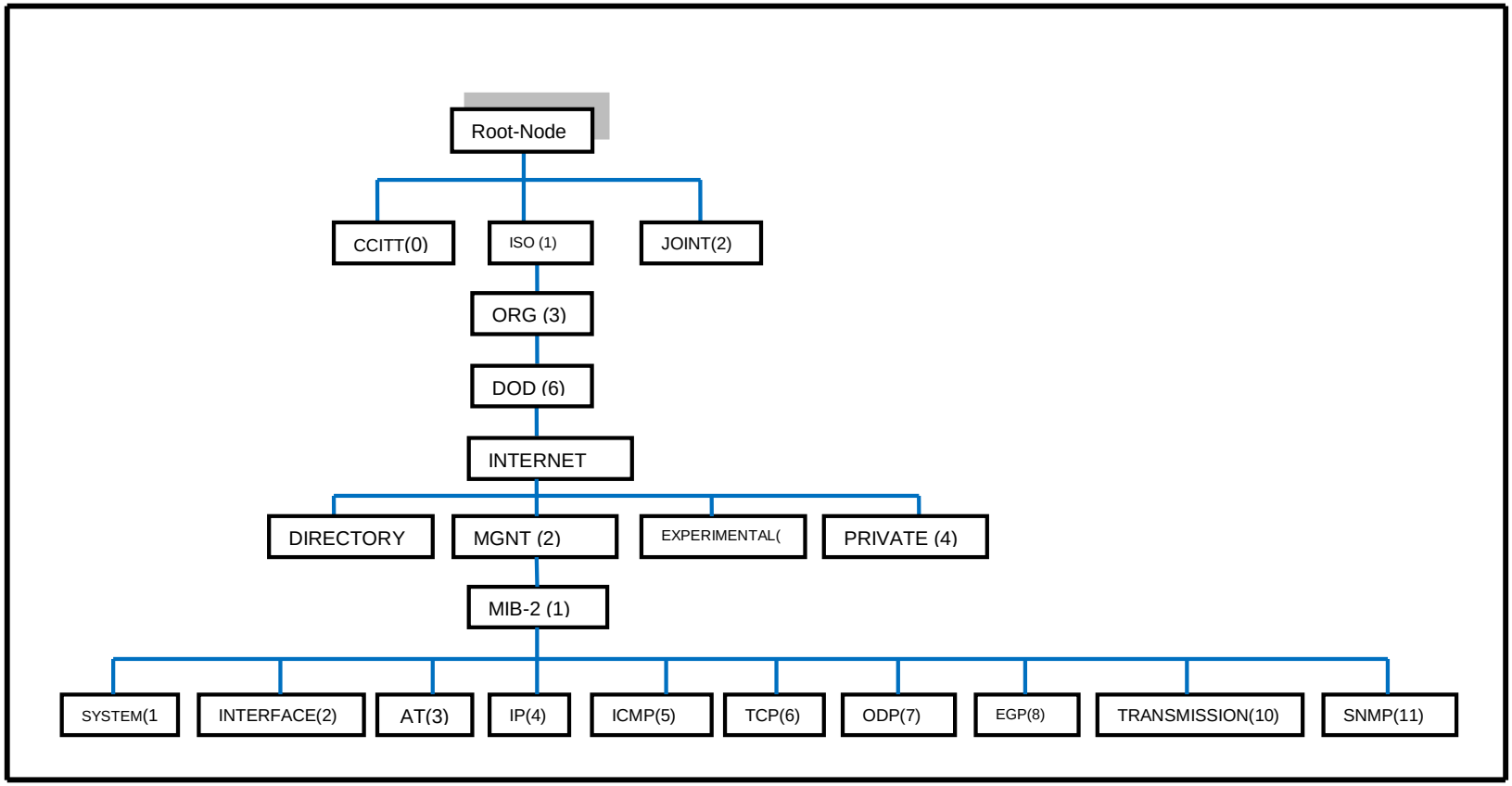



Figura 2.5 Estructura Jerárquica de Árbol MIB [26]

## 2.3 SNMPv3

En las versiones de SNMPv1 y SNMPv2 sus principales debilidades eran la seguridad de la transmisión de los mensajes entre el sistema gestor y el agente. La autenticación entre agente y gestor está basada en una clave el cual era enviado en texto plano. Esto representa un grave riesgo ya que el nombre de comunidad puede ser capturado, interpretado y utilizado para: obtener información de gestión desde los dispositivos de red, modificar parámetros de configuración o dar de baja a los dispositivos.

La creación de SNMPv3 resuelve las graves deficiencias existentes en las versiones anteriores. La seguridad es el principal tema tratado en SNMPv3 y no existen cambios significativos en el protocolo; se han introducidos nuevos conceptos, convenciones y terminologías que definen de manera precisa a los componentes ya conocidos de SNMP.

SNMPv3 es un protocolo de gestión de red que define una nueva arquitectura que ofrece seguridad de acceso a los dispositivos por medio de una combinación de autenticación y encriptación de los mensajes.

En la tabla 2.1 podemos observar las rfc`s en su versión más actualizada que sustentan el protocolo SNMPv3.

Tabla 2.1 RFC`s para SNMPv3 [24]

| NUMERO | NOMBRE |
|---|---|
| RFC 3411 | Arquitectura para sistemas SNMP |
| RFC 3412 | Despacho y procesamiento de mensajes SNMPv3 |
| RFC 3413 | Aplicaciones SNMPv3 |
| RFC 3414 | USM (User-based Security Model<br>Modelo de Seguridad basada en el Usuario) |
| RFC 3415 | VACM (View-based Access Control Model<br>Modelo de Control de Acceso basado en Vistas). |
| RFC 3416 | Operaciones de protocolo para SNMPv2 |
| RFC 3417 | Mapeo de transporte para SNMPv2 |
| RFC 3418 | MIBs para SNMPv2 |
| RFC 2576 | Coexistencia entre versiones de SNMP |
| RFC 2570 | Introducción a SNMPv3 |
| RFC 2786 | Administración de la llave Diffie-Hellman para USM |

### 2.3.1 Características de Seguridad.

[25] Este protocolo provee accesos de seguridad para los dispositivos de red, mediante la combinación de paquetes de autenticación y encriptación.

Y entre sus principales características están:

- Integridad: Cada mensaje SNMPv3 recibido será verificado para comprobar que no ha sido modificado durante su transmisión a través de la red de tal forma que una operación de gestión no autorizada pudiera llevarse a cabo.
- Autenticación: El protocolo deberá verificar la identidad del originador del mensaje recibido.
- Tiempo en que se originan los datos: El protocolo verifica el tiempo aparente de la generación del mensaje. Para proteger contra la amenaza de modificación de flujo de mensajes para lo cual una marca de tiempo es incluido en el mensaje.
- Confidencialidad: El protocolo deberá garantizar, cuando se ha necesario que el contenido del mensaje se ha indescifrable. Un algoritmo de encriptación es puesto en marcha para proteger contra la amenaza de revelación de contenido.

### 2.3.2 Modelos y niveles de Seguridad

[27] Tanto SNMPv1 como SNMPv2c emplean un esquema de seguridad basado en comunidades (comunity-strings) para establecer la autenticación entre un NMS y los Agentes. Las comunidades son esencialmente contraseñas, cadenas de texto que permiten a cualquier

aplicación basada en SNMP (y que conozca la cadena de texto) acceder a la información de gestión del dispositivo cliente o Agente.

El conjunto de dispositivos que pueden acceder a la MIB de un agente se define por una lista de control de acceso que relaciona las direcciones IP con una palabra clave, la comunidad.

Las estaciones administradoras se pueden configurar con tres tipos de permisos:

- De solo lectura (read-only): permite leer los valores de datos, pero deniega su modificación. Por ejemplo, permite leer el número de paquetes que se han transmitido a través de los puertos de un encaminado, pero no permite reiniciar este contador.
- De lectura-escritura (read-write): se permite leer los valores de los datos y realizar cambios en los elementos que tengan la propiedad de ser modificables.
- De notificación (trap): se permite recibir notificaciones por parte del Agente.

La versión 3 del protocolo define un nuevo modelo de seguridad, concretamente el Modelo de Seguridad de Usuario o USM (*User Security Model*). Este modelo proporciona las siguientes características:

- Integridad del mensaje: Garantizar que un paquete no ha sido alterado al recorrer la red.
- Autentificación: Determinar que el mensaje proviene de una fuente valida.
- Encriptación: Cifrar el contenido de un paquete a fin de evitar ser leído por una fuente no autorizada.

SNMPv3 proporciona tanto modelos como niveles de seguridad.

- Un modelo de seguridad es una estrategia de autenticación cuya configuración se basa en un usuario y al grupo al que pertenece.
- Un nivel de seguridad en el nivel permitido a un usuario dentro de un modelo de seguridad.

La combinación de un modelo de seguridad y un nivel de seguridad determina el mecanismo de seguridad que se emplea a la hora de manejar paquetes-SNMP.

La tabla 2.2 detalla los modelos y niveles de seguridad en cada una de las versiones SNMP.

Tabla 2.2 Modelos y Niveles de Seguridad [27]

| Versión | Descripción | Autenticación | Encriptación | Nivel |
|---|---|---|---|---|
| SNMPv1 | Usa el modelo basado en comunidades | Community string | No | No autenticación No encriptación |
| SNMPv2, SNMPv2c | Usa el modelo basado en comunidades | Community string | No | No autenticación No encriptación |
| SNMPv3 | Utiliza nombres de usuarios para comprobar la autenticación. | USM (User Security Model) | No | No autenticación No encriptación |
| SNMPv3 | Variante de SNMPv3 que provee una autenticación basada en los algoritmos de HMAC-SHA o HMAC-MD5 | USM + MD5 o SHA | No | Autenticación No Encriptación |
| SNMPv3 | Configuración más segura de SNMPv3 que provee algoritmos de autenticación y encriptación DES de 56 bits | USM+MD5 o SHA | DES | Autenticación Encriptación |

### 2.3.3 Arquitectura SNMPv3

[25] En SNMPv3 no existe el concepto de gestores y agentes. Ambos, administradores y agentes, ahora se denominan entidades SNMP**.** Cada entidad está formada por un único motor SNMP y por una o más aplicaciones SNMP. El motor y las aplicaciones a su vez están formados por diferentes subsistemas o módulos. Los subsistemas a su vez están conformados por modelos. Los subsistemas interactúan entre sí mediante primitivas y parámetros abstractos con el fin de que una entidad pueda proveer un determinado servicio. Dependiendo de los tipos de módulos que conformen una entidad, esta podrá actuar como: agente, gestor o una combinación de ambos.

La arquitectura SNMP tiene algunas ventajas:

- Permite el desarrollo de estrategias de coexistencia y transición con otros módulos.
- Definición del rol de una entidad en base a los módulos que se tenga implementado.
- Capacidad de actualizar de forma modular sin la necesidad de actualizar todo el protocolo.

### 2.3.4 Entidades SNMP

[28] Es un conjunto de módulos que interactúan entre sí. Cada entidad SNMP ofrece una porción de la capacidad de SNMP y puede actuar como los tradicionales Agentes o gestores o una combinación de ambos. Cada entidad está formada por módulos que interactúan entre sí para ofrecer un servicio, como se ilustra en la figura 2.2.

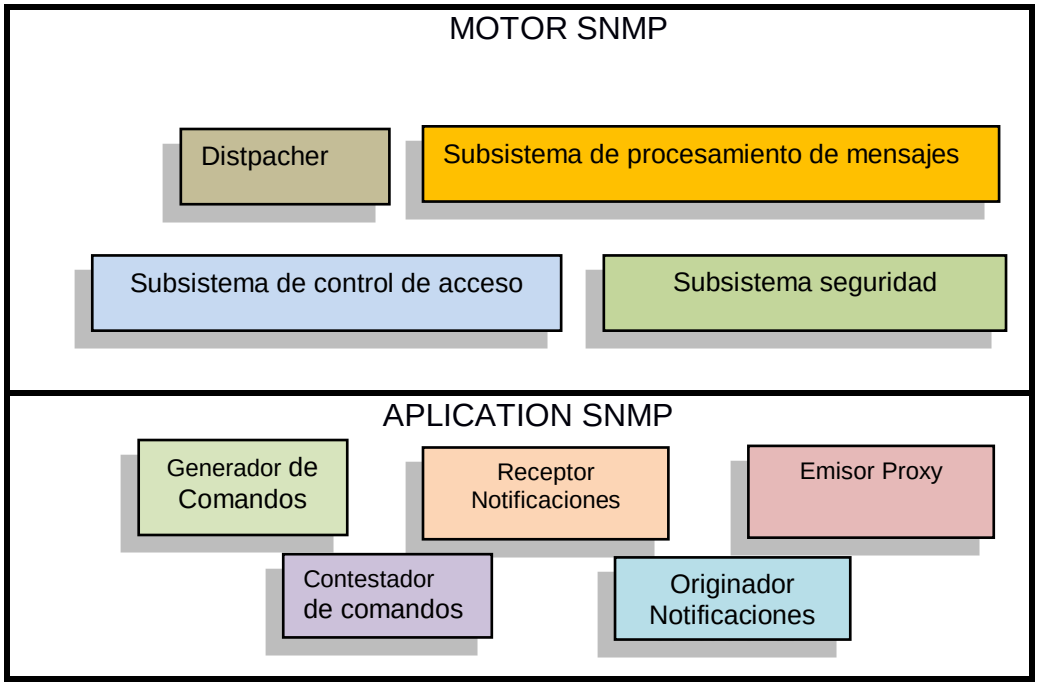



Figura 2.2 Entidad SNMPv3 [24]

Motor SNMP

Es la parte esencial de cualquier entidad SNMP.

El Motor SNMP es el encargado de proporcionar las funciones de.

- Envió de mensajes
- Recepción de mensajes
- Autenticación
- Encriptado y desencriptado de los mensajes
- Control de Acceso a los objetos administrados

Estas funciones son provistas como servicios a una o más aplicaciones y está provisto de 4 módulos.

**Dispatcher (Despachador)**

Es el encargado de administrar el tráfico. Para mensajes salientes recibe las PDUs de las aplicaciones. Determina el tipo de procesamiento requerido (SNMPv1, SNMPv2, SNMPv3) y entrega estos datos al módulo de procesamiento de mensajes adecuado.

**Subsistema de Procesamientos Mensajes**

Es el responsable del armado y desarmado de la PDU, recibe y entrega los mensajes del despachador.

**Subsistema de Seguridad**

Es el encargado de ejecutar las funciones de autenticación y encriptación de los mensajes SNMP, haciendo uso del modelo de seguridad basado en usuarios (USM), agregando un encabezado especifico de seguridad en cada mensaje.

**Subsistema de Control de Acceso.**

Proporciona servicios de autorización para controlar el acceso a los objetos MIB, es decir determina a que objetos de la MIB se accede y que operaciones pueden ejecutarse en ellos.

**Aplicaciones SNMP**

Las aplicaciones SNMP son subsistemas que usan los servicios de un motor SNMP para llevar a cabo operaciones especificas relacionadas al procesamiento de información de gestión.

**Generador de Comandos**

Monitoriza y maneja los datos de administración de los dispositivos. Especialmente genera las PDUs: GetRequest, GetNextRequest, GetBulkRequest y SetRequest, además recibe y procesa las respuestas GetResponse a los pedidos que ha generado. Esta aplicación se implementa en la entidad que actúa como NMS.

**Contestador de comandos**

Recibe las PDUs GetRequest, GetNextRequest, GetBulkRequest y SetRequest, realiza las acciones solicitadas y utilizando el control de acceso, genera mensajes GetResponse para responder la solicitud de una NMS. Esta aplicación es implementada en una estación que actúa como agente.

**Receptor de Notificaciones**

Es el encargado de monitorizar la llegada de notificaciones y de tratarlas una vez recibidas y en el caso de un InformTequest genera un Getresponse.

**Generador de Notificaciones**

El encargado de monitorizar constantemente el sistema y de generar las notificaciones, en caso de detectar un evento particular, que haya cambiado la forma de operar del dispositivo monitoreado.

**Reenviador Proxy**

Reenvía mensajes entre entidades SNMP. La implementación de esta aplicación es opcional. Una entidad no tiene por qué implementar todos los módulos anteriores ya que esto depende de las funcionalidades que se desea que tenga dispositivo.

### 2.3.5 Agente SNMPv3

Una entidad SNMP que contenga una o más aplicaciones contestadoras de comandos, originadoras de notificaciones y opcionalmente reenviadores proxy (junto con un motor SNMP) se llama agente SNMP.

El motor SNMP de un agente SNMP contiene los subsistemas del motor de un Gestor SNMP más un subsistema de control de acceso.

### 2.3.6 Formato mensaje SNMPv3

El formato de un mensaje SNMPv3 cambia respecto a las dos versiones anteriores en virtud de que debe involucrar parámetros para el proceso de autenticación y encriptación. En la figura 2.3 se podrá observar el formato de un mensaje SNMPv3.

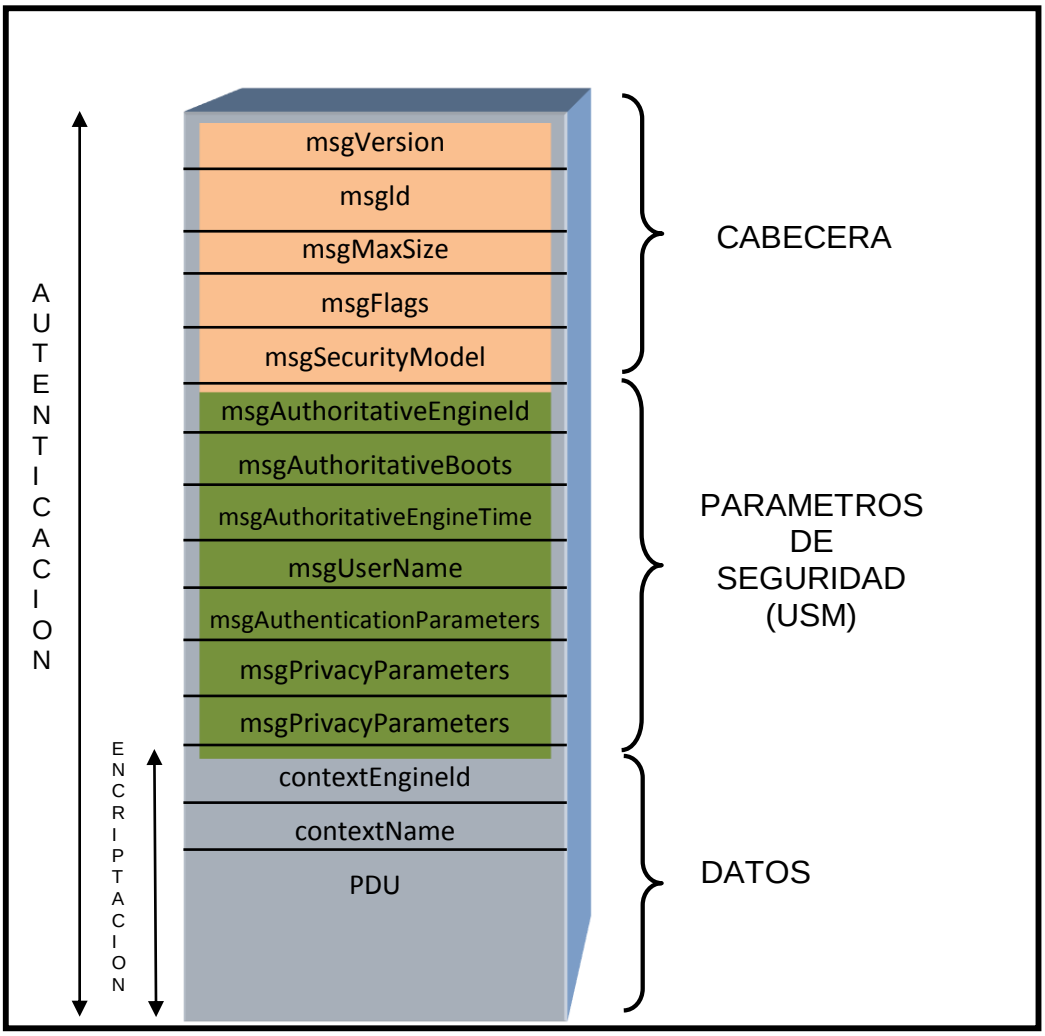



Figura 2.3 Formato de un mensaje SNMPv3 [25]

- msgVersion: Indica la versión de SNMP
- msgId: Numero de 32 bits que sirve para relacionar las peticiones con las respuestas.
- msgMaxSize: Numero de 32 bits que indica la cantidad en bytes que puede recibir el emisor del mensaje.
- msgFlags: Numero de 8 bits, pero solo usa los 3 bits menos significativos para indicar el nivel de seguridad a emplear:

    - reportableFlag: El valor 1 en este subcampo indica que el receptor del mensaje debe enviar de vuelta un acuse de recibo.
    - privFlag: El valor 1 indica que se debe encriptar el mensaje.
    - authFlag: Cuando se asigna el valor 1 se debe aplicar autenticación al mensaje.

- msgSecurityModel: Indica el modelo de seguridad empleado para la emisión del mensaje. SNMPv1 (1), SNMPv2 (2) Y USM de SNMPv3 (3).

La siguiente sección contiene parámetros exclusivos para la operación de USM:

- msgAutoritativeEngineID: Es un identificador que se asigna al motor de una entidad SNMP (agente o gestor) que responde a las peticiones o al que recibe las notificaciones, y que es el que sirve como referencia para el control de la sincronización entre agente y gestor. A este motor se lo denomina Motor Autorizado (AutoritativeEngine).
- msgAuthoritativeEngineBoots: Indica el número de ocasiones que un motor SNMP reinicio desde su configuración original.
- msgAutoritativeEngineTime. Indica el tiempo en segundos desde que inicio por última vez.
- msgUserName: Indica el nombre de usuario que envía la petición o respuesta.
- msgAuthenticationParameters: En el caso en que se aplique autenticación este campo contiene el código de autenticación HMAC.
- msgPrivacyParameters: En el caso en que se aplique encriptación contiene el vector inicial (VI) para el proceso de desencriptacion DES-CBC.

La tercera sección es la que contiene la PDU SNMP definidas en la versión 2.

Contiene los siguientes campos:

- contextEngineId: Es el identificador de una entidad SNMP asociado a un contexto.
- contextName: Nombre que se asigna a un contexto.
- PDU: Contiene los valores (OID e instancias) de una petición o respuesta SNMP.

### 2.3.7 Seguridad en SNMPv3

[29] La Seguridad esta descripta en el subsistema de Seguridad que ejecuta funciones de autenticación y encriptado, para las mismas define los Modelos de Seguridad de Usuario (USM). Específicamente la RFC 3414 establece que este modelo protege contra lo siguiente:

- Modificación de Información.
- Falsificación de entidad.
- Modificación de mensaje.
- Difusión de Información.

También aclara que no protege contra ataques de negación de servicio ni análisis de tráfico.

Este modelo se emplea para proveer autenticación y privacidad, para esto define dos claves, una clave privada (PrivKey) y otra de autenticación (AutKey). El valor de estas claves no es accesible vía SNMP y se emplean de la siguiente forma:

**Autenticación**:

Se definen dos alternativas para esta tarea, HMAC-MD5-96 Y HMAC-SHA-96.

La mecánica de esta función es que a través de una cadena de bit de entrada de cualquier longitud finita, generara un único resumen de salida de longitud fija. Que en el caso de esta norma es de 20 Byte para SHA o 16 Byte para MD5.

Esta función llamada “One Way” pues no es posible a través del resumen de salida obtener el texto de entrada, también resultara computacionalmente imposible obtener un valor de salida igual a través de otro valor de entrada, como así tampoco desde un valor de salida ya calculado, obtener otro valor de entrada diferente al verdadero.

La aplicación aquí propuesta toma los datos y la clave y produce un resumen:

- Resumen=H (clave, datos).

En cualquiera de los dos casos, se toman como válidos los primeros 96 bits, descartando el resto.

**Criptografía:**

Para esta actividad USM emplea el algoritmo DES (Data Encryptation Standard) [ANSI X3.106] en el modo cifrado encadenado de bloque (CBC).

La clave privada (PrivKey) antes mencionada de longitud 16 byte es empleada aquí dividiéndola en dos, los primeros 8 Byte, es decir 64 bit son empleados como clave para DES, el cual solo tendrá en cuenta 56, dejando 8 para control de paridad. Los últimos 8 Byte son empleados como Vector de Inicialización (IV) para comenzar con el cifrado en cadena.

Esta técnica CBC, se basa en tomar el primer bloque de texto plano, y realizar una operación XOR con un Vector de inicialización y luego de esta operación recién se pasara al cifrado de ese bloque. En el segundo bloque se realizara nuevamente la operación XOR, pero esta vez será el texto plano de este bloque con el bloque cifrado anteriormente, y luego se cifrara. Esta mecánica se irá realizando en los sucesivos bloques, es decir XOR con el bloque cifrado anterior y luego cifrado.

El descifrado se realiza en forma inversa.

- Cifrado = E (clave, texto).
- D (clave, cifrado) = texto.

Localización de claves:

Una clave localizada es un secreto compartido entre un usuario y un motor SNMP autoritativo.

El problema del empleo de una sola clave por parte del usuario con todos los agentes es que si se descubriera la misma, seria vulnerable todo el sistema. Si el caso fuera lo contrario es decir que se deseara

emplear una clave distinta para cada agente, entonces el usuario debería recordar todas las contraseñas lo cual en la práctica no es viable.

Para dar solución a estos problemas la RFC 3414 propone este proceso por el cual una clave única de usuario (o pueden ser dos: una para privacidad y otra para autenticación) es convertida a múltiples claves únicas también, una para cada motor SNMP, este proceso es lo que se denomina Localización de Claves.

Las características fundamentales que propone este proceso son:

- Cada agente SNMP tiene su propia clave única para cada usuario autorizado, por lo tanto si la clave de uno de ellos es comprometida, no lo serán las del resto.

- La clave de un usuario es diferente en cada agente SNMP, por lo tanto si se compromete la clave de un agente, no comprometerá al resto ni a la clave del usuario.

- La administración de la red, puede realizarse en forma segura remotamente desde cualquier punto de la red.

# CAPÍTULO 3

## 3 DISEÑO DE LA RED BANCARIA

### 3.1 Diseño físico de la Red Bancaria

El presente modelo piloto puede ser aplicado a cualquier institución bancaria; su infraestructura se compone de la interconexión de una red de datos desde la casa matriz (para efectos de la implementación, se asume ubicada en la ciudad de Guayaquil) hacia cada una de las diferentes agencias y sucursales, repartidas en diversos sectores de la ciudad y en distintas ciudades del país.

El objetivo de este análisis es la implementación de una red WAN IPv6, que permita conectar a la Red LAN de la Casa Matriz con sus diferentes Agencias y Sucursales además de poder gestionar su infraestructura.

La implementación de la red IPv6 está enmarcada dentro de un proyecto de gestión de infraestructura de Red en forma segura. Esta implementación se debe a la necesidad creciente de mayor seguridad en la transmisión y recepción de información de las diferentes transacciones bancarias.

### 3.1.1 Infraestructura de la Red Bancaria.

La infraestructura de la presente Red Bancaria Piloto debe soportar soluciones convergentes de Voz, Datos, Video, Seguridad y futuros servicios que se brindará.

Esta infraestructura está basada primeramente en un buen tendido de Cableado Estructurado, tanto en el edificio Central como en las Agencias e Islas de atención a los usuarios. Además de la Seguridad Física implementada con el objetivo de proteger el acceso no

autorizado hacia los equipos de la red de datos en cada una de nuestras agencias y/o sucursales.

El cableado estructurado de cada una de nuestras agencias y/o sucursales está implementado siguiendo las normas ANSI/TIA/EIA; no vamos a ahondar sobre el tendido, lo asumimos implementado completamente.

Nos fijaremos en el diseño y los equipos que conforman la Red Lan-WiFi y WAN Segura, basados en los estándares de cumplimiento de la Industria de Tarjetas de Pago o “PCI Compliance” por sus siglas en Ingles (Payment Card Industry Compliance).

La red LAN está conformada por un conmutador Principal Core con capacidad de Routing, y switches de Distribución para las diferentes Vlan del Banco. Cada conmutador de Distribución a su vez lleva a conmutadores de acceso para los usuarios Finales.

Los servidores, que están repartidos en equipos Blade, como Máquinas Virtuales o “Virtual Machines” (VM) por sus siglas en Ingles, repartidas en los diferentes segmentos o Vlans.

Las maquinas PC de los usuarios finales que ejecutan las acciones del trabajo diario de cada departamento separado por pisos, entre ellos están los usuarios VIP o Gerentes, con los diferentes roles asignados para el Trabajo.

Cada segmento de Red del Banco está protegido por Firewalls/IPS, los Firewalls/IPS están destinados para permitir, denegar y filtrar el tráfico desde y hacia los diferentes segmentos o Vlans del Banco entre ellas el Centro de Cómputo.

Se usa un Firewall de Aplicaciones Web o WAF (Web Aplication Firewall) por sus siglas en Ingles. Basado en Reglas nos ayuda a proteger a los servidores WEB desde los más comunes ataques a los protocolos WEB como también los más complejos.

Balanceo de servidores, se usa para balancear la carga de Servidores transaccionales, sobre todo con los servidores WEB.

Enrutadores se usan para interconectar la red del Banco (Centro de Computo) con la Internet, la WAN del Banco, y los servicios de los asociados y proveedores externos, tales como el Banco Central; la

Superintendencia de Bancos, Otros Bancos, Administradores de Tarjetas de Crédito, Telefónicas, las Representaciones Internacionales de nuestro Banco.

La figura 3.1 Detalla la infraestructura de la Red LAN típica de una Institución Bancaria.

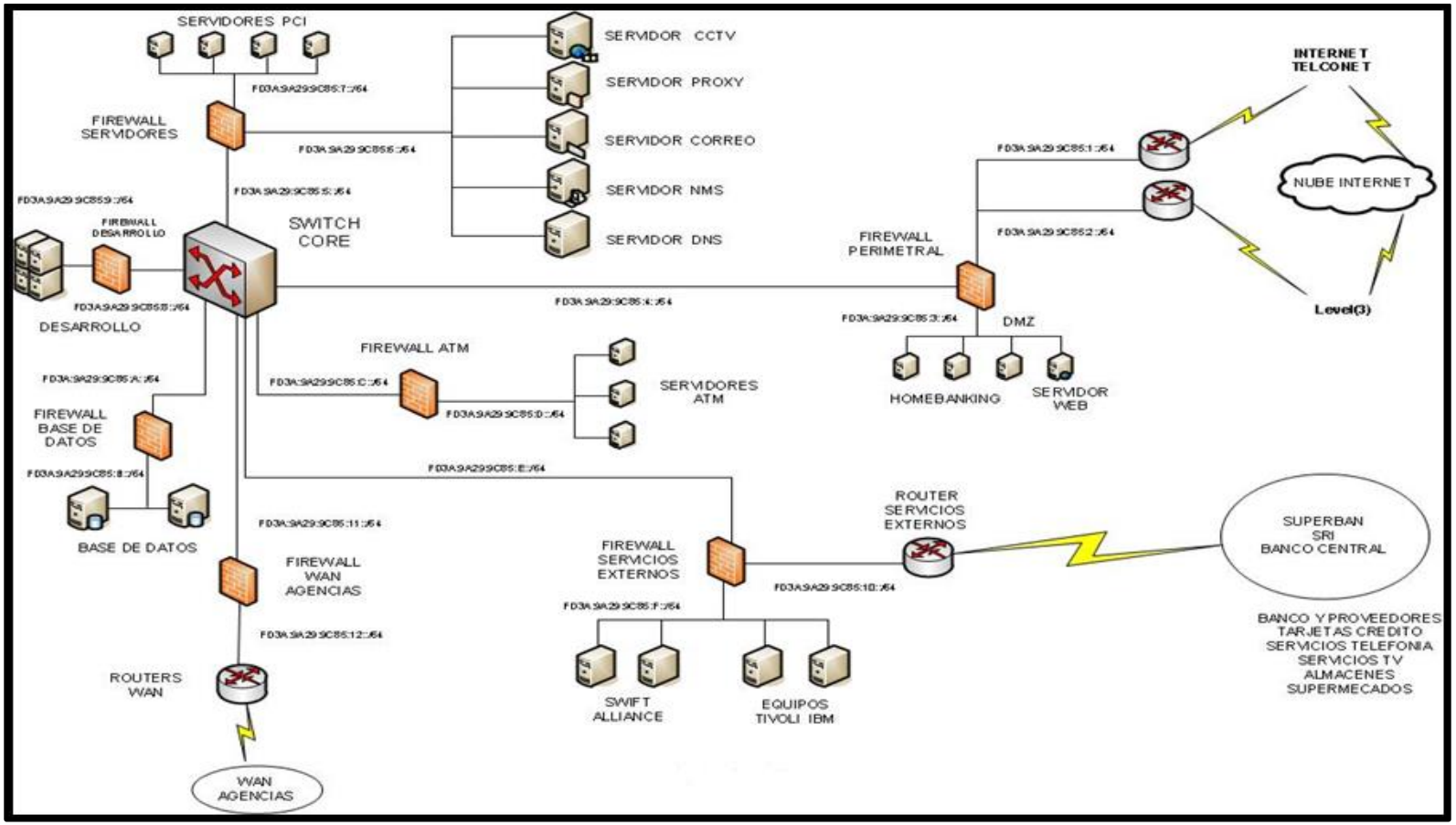



Figura 3.1 Infraestructura de Red Bancaria

## 3.2 Diseño lógico de la Red Bancaria

### 3.2.1 Diseño de la topología de La Red

La topología de la Red WAN del Banco que será materia de estudio, tendrá un enrutador Central que hará de enrutador principal y que permitirá la conexión entre las diversas sucursales y agencias hacia la matriz.

La topología usada en la Red Bancaria es del tipo Estrella Extendida, que me permitirá seguir creciendo de acuerdo a mis requerimientos de crecimiento futuro.

La figura 3.2 Muestra en detalle la Red WAN que será materia de nuestro estudio.

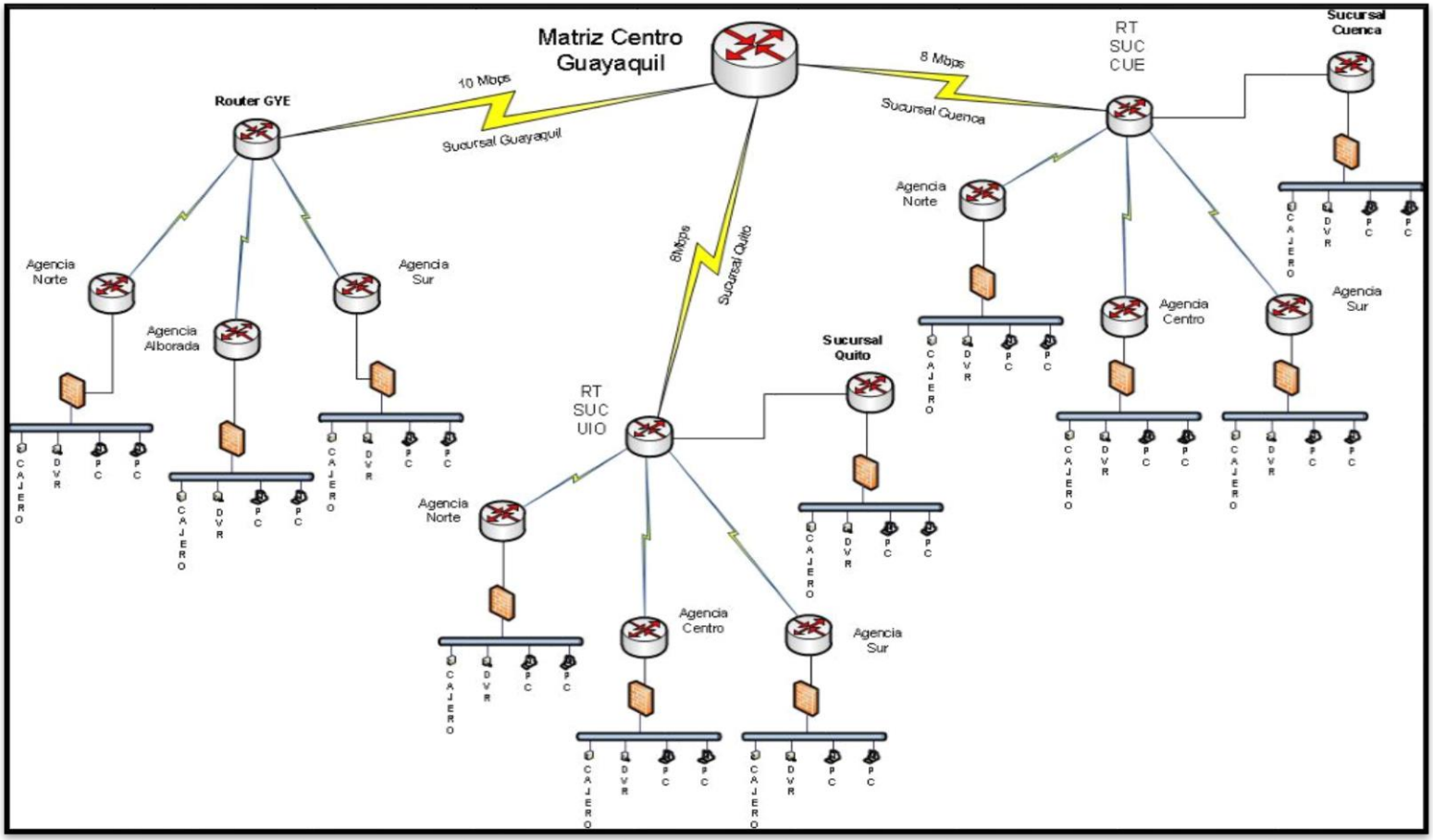



Figura 3.2 Esquema de Conexión WAN entre Agencias

### 3.2.2 Diseño del modelo de Direccionamiento.

#### 3.2.2.1 Direccionamiento Protocolo de Internet Versión 6 (IPv6).

El prefijo que se optó para esta simulación del proyecto de implementación de una red bancaria, se lo obtuvo siguiendo el esquema de direcciones Unique Local Unicast. La figura 3.3 detalla el formato de la dirección Unique Local Unicast.

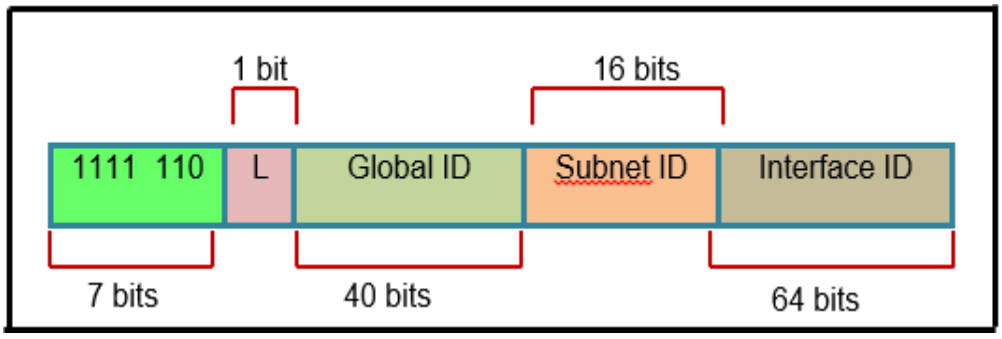



Figura 3.3 Formato de Dirección Unique Local Unicast. [8]

| Binario | | | Hexadecimal |
|---|---|---|---|
| 1111 | = | | F |
| 110L | L=1 | 1101 | D |
| | L=0 | 1100 | C |

Global ID

Se la obtiene de forma seudo-aleatoria siguiendo los pasos establecidos en la RFC 4193.

- Obtener la hora del día actual de 64 bits en formato Network Time Protocol (NTP).

- Obtener una EUI-64 Identificador del funcionamiento de este sistema algoritmo. Si un EUI-64 no se puede obtener o no puede ser creado un identificador convenientemente único local para el nodo, se debe utilizar (por ejemplo, el sistema de número de serie).

- Concatenar la hora del día con el sistema específico de identificación, con el fin de crear una clave.

- Calcular un SHA-1 compendio sobre la clave. El valor resultante es de 160 bits.

- Use los 40 bits menos significativos como la global ID.

- Concatenar FC00::/7, la L igual a 1, y la de 40 bits Mundial ID de crear una dirección IPv6 prefijo local.

Este algoritmo se traducirá en un identificador Global ID único, y puede utilizarse para crear un prefijo IPv6 de uso local.

Para calcular nuestro Unique Local Unicast usaremos herramientas computacionales existentes en el internet que nos permiten crear nuestro Global ID de 40 bits y me mostrara una subred lista para su uso. En el link http://bitace.com/ipv6calc/ se podrá obtener una generación rápida de una dirección Unique Local Adress.

La Subred escogida para nuestro estudio es la siguiente:

**FD3A:9A29:9C85::/48**

Siendo la red Bancaria un usuario final una red de prefijo /48 sería el prefijo ideal.

El prefijo FD3A:9A29:9C85::/48 permite disponer de 16 bits para realizar un sub-netting y tener una mayor cobertura nacional.

Con el objetivo de realizar una correcta distribución del gran número de direcciones disponibles, se optó por implementar una política de direccionamiento jerárquico que considera a las distintas provincias y ciudades del ecuador, como se muestra en la tabla 3.1.

Tabla 3.1 Estructura direcciones IPv6

| Nombre Campo | FD3A:9A29:9C85::/48 | Provincia | Ciudad | Sub-Red | Dispositivo (Interfaz) |
|---|---|---|---|---|---|
| Tamaño Campo | 48[bit] | 4[bit] | 4[bit] | 8[bit] | 64[bit] |
| Prefijo | /48 | /52 | /56 | /64 | /128 |

La figura 3.4 muestra cómo está diseñado el esquema de direccionamiento IPv6 en la Red WAN

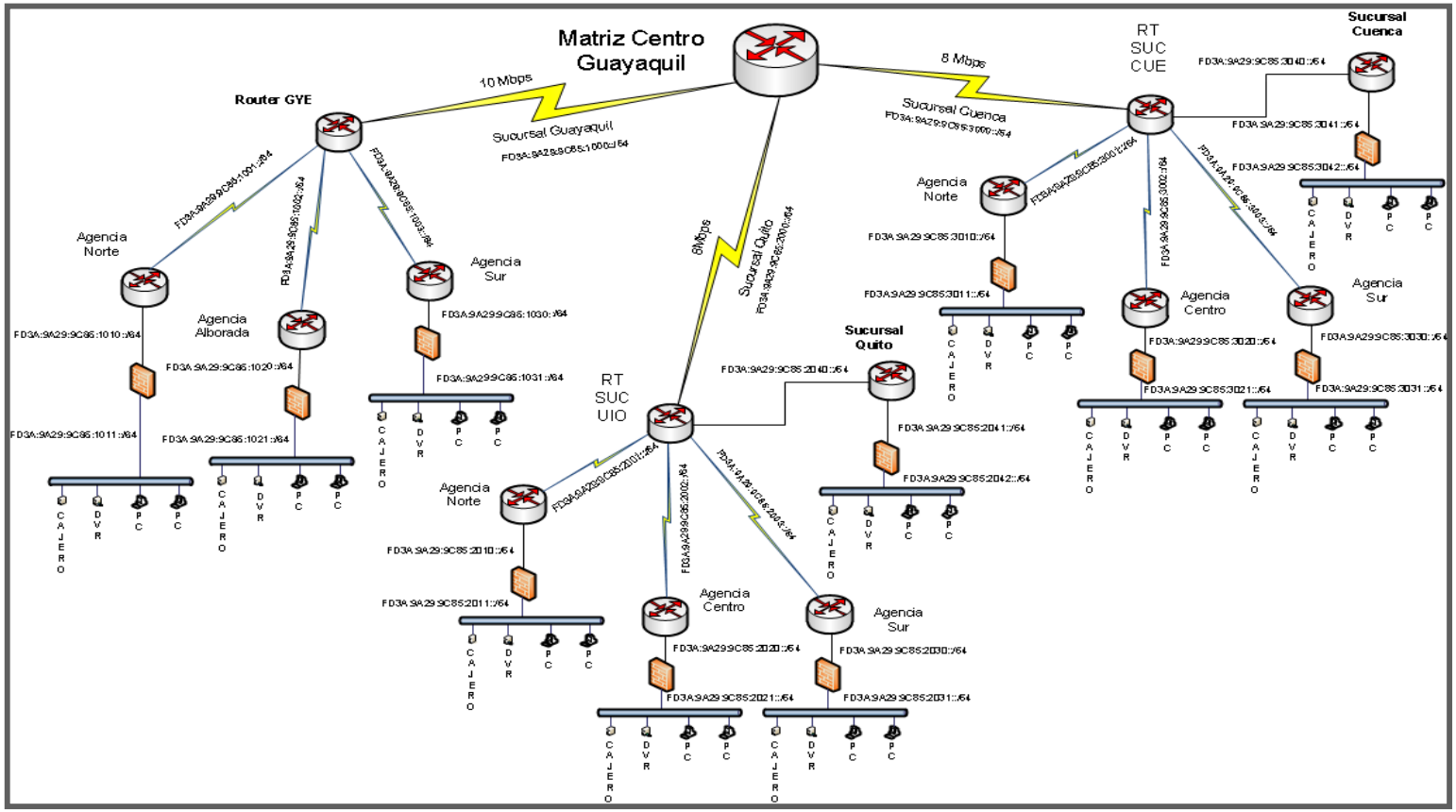



Figura 3.4 Esquema de Direccionamiento WAN

Las tablas 3.2 y 3.3 detallan las asignaciones de direcciones IPv6 en nuestra Institución Bancaria.

Tabla 3.2 Asignaciones de Direcciones IPv6

| ESQUEMA DE ASIGNACION | | | FD3A:9A29:9C85::/48 |
|---|---|---|---|
| | | | |
| NUMERO | DIRECCION DE RED | PREFIJO | DESCRIPCION |
| 1 | FD3A:9A29:9C85:0000:: | 52 | MATRIZ |
| 2 | FD3A:9A29:9C85:1000:: | 52 | PROVINCIA GUAYAS |
| 3 | FD3A:9A29:9C85:2000:: | 52 | PROVINCIA DEL PICHINCHA |
| 4 | FD3A:9A29:9C85:3000:: | 52 | PROVINCIA DEL AZUAY |
| 5 | FD3A:9A29:9C85:4000:: | 52 | PROVINCIA EL ORO |
| 6 | FD3A:9A29:9C85:5000:: | 52 | PROVINCIA DE ESMERALDAS |
| 7 | FD3A:9A29:9C85:6000:: | 52 | PROVINCIA DE LOJA |
| 8 | FD3A:9A29:9C85:7000:: | 52 | USO FUTURO |
| 9 | FD3A:9A29:9C85:8000:: | 52 | USO FUTURO |
| 10 | FD3A:9A29:9C85:9000:: | 52 | USO FUTURO |
| 11 | FD3A:9A29:9C85:A000:: | 52 | USO FUTURO |
| 12 | FD3A:9A29:9C85:B000:: | 52 | USO FUTURO |
| 13 | FD3A:9A29:9C85:C000:: | 52 | USO FUTURO |
| 14 | FD3A:9A29:9C85:D000:: | 52 | USO FUTURO |
| 15 | FD3A:9A29:9C85:E000:: | 52 | USO FUTURO |
| 16 | FD3A:9A29:9C85:F000:: | 52 | USO FUTURO |

Tabla 3.3 Asignaciones de Segmentos de Red IPv6

| ESQUEMA DE ASIGNACION | | | FD3A:9A29:9C85:0000::/52 |
|---|---|---|---|
| NUMERO | DIRECCION DE RED | PREFIJO | DESCRIPCION |
| MATRIZ | | | FD3A:9A29:9C85:0000::/56 |
| 1 | FD3A:9A29:9C85:0001:: | 64 | PROVEEDOR DE INTERNET A |
| 2 | FD3A:9A29:9C85:0002:: | 64 | PROVEEDOR DE INTERNET B |
| 3 | FD3A:9A29:9C85:0003:: | 64 | SERVIDORES DMZ |
| 4 | FD3A:9A29:9C85:0004:: | 64 | FIREWALL PERIMETRAL |
| 5 | FD3A:9A29:9C85:0005:: | 64 | FIREWALL SERVIDORES PCI |
| 6 | FD3A:9A29:9C85:0006:: | 64 | SERVIDORES INTERNOS |
| 7 | FD3A:9A29:9C85:0007:: | 64 | SERVIDORES PCI |
| 8 | FD3A:9A29:9C85:0008:: | 64 | FIREWALL DESARROLLO |
| 9 | FD3A:9A29:9C85:0009:: | 64 | SERVIDORES DESARROLLO |
| 10 | FD3A:9A29:9C85:000A:: | 64 | FIREWALL BASE DE DATOS |
| 11 | FD3A:9A29:9C85:000B:: | 64 | SERVIDORES BASE DE DATOS |
| 12 | FD3A:9A29:9C85:000C:: | 64 | FIREWALL ATM |
| 13 | FD3A:9A29:9C85:000D:: | 64 | SERVIDORES ATM |
| 14 | FD3A:9A29:9C85:000E:: | 64 | FIREWALL SERVICIOS EXTERNOS |
| 15 | FD3A:9A29:9C85:000F:: | 64 | SERVIDORES SERVICIOS EXTERNOS |
| 16 | FD3A:9A29:9C85:0010:: | 64 | ROUTER SERVICIOS EXTERNOS |
| 17 | FD3A:9A29:9C85:0011:: | 64 | FIREWALL WAN AGENCIAS |
| 18 | FD3A:9A29:9C85:0012:: | 64 | ROUTER WAN AGENCIAS |

| ESQUEMA DE ASIGNACION | FD3A:9A29:9C85:1000::/52 |
|---|---|

| NUMERO | DIRECCION DE RED | PREFIJO | DESCRIPCION |
|---|---|---|---|
| PROVINCIA DEL GUAYAS | | | FD3A:9A29:9C85:1000::/56 |
| 19 | FD3A:9A29:9C85:1000:: | 64 | ROUTER WAN GYE |
| 20 | FD3A:9A29:9C85:1001:: | 64 | ENLACE WAN AGENCIA NORTE |
| 21 | FD3A:9A29:9C85:1002:: | 64 | ENLACE WAN AGENCIA ALBORADA |
| 22 | FD3A:9A29:9C85:1003:: | 64 | ENLACE WAN AGENCIA SUR |
| 23 | FD3A:9A29:9C85:1010:: | 64 | FIREWALL AGENCIA NORTE |
| 24 | FD3A:9A29:9C85:1011:: | 64 | RED LAN AGENCIA NORTE |
| 25 | FD3A:9A29:9C85:1020:: | 64 | FIREWALL AGENCIA ALBORADA |
| 26 | FD3A:9A29:9C85:1021:: | 64 | RED LAN AGENCIA ALBORADA |
| 27 | FD3A:9A29:9C85:1030:: | 64 | FIREWALL AGENCIA SUR |
| 28 | FD3A:9A29:9C85:1031:: | 64 | RED LAN AGENCIA SUR |

| ESQUEMA DE ASIGNACION | FD3A:9A29:9C85:2000::/52 |
|---|---|

| NUMERO | DIRECCION DE RED | PREFIJO | DESCRIPCION |
|---|---|---|---|
| PROVINCIA DE PICHINCHA | | | FD3A:9A29:9C85:2000::/56 |
| 29 | FD3A:9A29:9C85:2000:: | 64 | ROUTER WAN QUITO |
| 30 | FD3A:9A29:9C85:2001:: | 64 | ENLACE WAN AGENCIA NORTE |
| 31 | FD3A:9A29:9C85:2002:: | 64 | ENLACE WAN AGENCIA CENTRO |
| 32 | FD3A:9A29:9C85:2003:: | 64 | ENLACE WAN AGENCIA SUR |
| 33 | FD3A:9A29:9C85:2040:: | 64 | ENLACE WAN SUCURSAL QUITO |
| 34 | FD3A:9A29:9C85:2010:: | 64 | FIREWALL AGENCIA NORTE |
| 35 | FD3A:9A29:9C85:2011:: | 64 | RED LAN AGENCIA NORTE |
| 36 | FD3A:9A29:9C85:2020:: | 64 | FIREWALL AGENCIA CENTRO |
| 37 | FD3A:9A29:9C85:2021:: | 64 | RED LAN AGENCIA CENTRO |
| 38 | FD3A:9A29:9C85:2030:: | 64 | FIREWALL AGENCIA SUR |
| 39 | FD3A:9A29:9C85:2031:: | 64 | RED LAN AGENCIA SUR |
| 40 | FD3A:9A29:9C85:2041:: | 64 | FIREWALL SUCURSAL QUITO |
| 41 | FD3A:9A29:9C85:2042:: | 64 | RED LAN SUCURSAL QUITO |

| ESQUEMA DE ASIGNACION | FD3A:9A29:9C85:3000::/52 |
|---|---|

| NUMERO | DIRECCION DE RED | PREFIJO | DESCRIPCION |
|---|---|---|---|
| PROVINCIA DEL AZUAY | | | FD3A:9A29:9C85:3000::/56 |
| 42 | FD3A:9A29:9C85:3000:: | 64 | ROUTER WAN CUENCA |
| 43 | FD3A:9A29:9C85:3001:: | 64 | ENLACE WAN AGENCIA NORTE |
| 44 | FD3A:9A29:9C85:3002:: | 64 | ENLACE WAN AGENCIA CENTRO |
| 45 | FD3A:9A29:9C85:3003:: | 64 | ENLACE WAN AGENCIA SUR |
| 46 | FD3A:9A29:9C85:3040:: | 64 | ENLACE WAN SUCURSAL CUENCA |
| 47 | FD3A:9A29:9C85:3010:: | 64 | FIREWALL AGENCIA NORTE |
| 48 | FD3A:9A29:9C85:3011:: | 64 | RED LAN AGENCIA NORTE |
| 49 | FD3A:9A29:9C85:3020:: | 64 | FIREWALL AGENCIA CENTRO |
| 50 | FD3A:9A29:9C85:3021:: | 64 | RED LAN AGENCIA CENTRO |
| 51 | FD3A:9A29:9C85:3030:: | 64 | FIREWALL AGENCIA SUR |
| 52 | FD3A:9A29:9C85:3031:: | 64 | RED LAN AGENCIA SUR |
| 53 | FD3A:9A29:9C85:3041:: | 64 | FIREWALL SUCURSAL QUITO |
| 54 | FD3A:9A29:9C85:3042:: | 64 | RED LAN SUCURSAL QUITO |

### 3.2.3 Enrutamiento de la red Bancaria con Protocolo de Internet Versión 6 (IPv6).

El protocolo de enrutamiento que se escogió para implementar en nuestro proyecto es el Open Shortest Path First versión 3 (OSPFv3), que es un protocolo de enrutamiento para las versiones IPv4 e IPv6. Es un protocolo de estado de enlace, en lugar de un protocolo por vector de distancia. OSPFv3 se describe en el RFC 5340 y es compatible para los protocolos IPv6 e IPv4.

Un protocolo de estado de enlace toma sus decisiones de enrutamiento basadas en los estados de los enlaces que conectan las máquinas de origen y destino.

Con el fin de garantizar que los paquetes OSPFv3 no se alteren y se reenvíen al enrutador, haciendo que el enrutador se comporte de una manera no deseada por los administradores de sistemas, los paquetes OSPFv3 deben ser autenticados. OSPFv3 usa la (*Application Program Interface*) API de socket seguro, el uso de IPsec añade autenticación a los paquetes OSPFv3.

Esta API es compatible con IPv6. OSPFv3 requiere el uso de IPsec para habilitar la autenticación. Las imágenes Criptográficas están obligadas a utilizar la autenticación, ya que sólo las imágenes incluyen la API de cifrado IPsec necesaria para el uso con OSPFv3.

Cuando OSPFv3 funciona con IPv6, OSPFv3 requiere el encabezado de autenticación de IPv6 (AH) o de la cabecera (ESP) para asegurar la integridad, autenticidad y confidencialidad de los intercambios de enrutamiento. En IPv6 las cabeceras de extensión AH y ESP se pueden utilizar para proporcionar autenticación y la confidencialidad a OSPFv3.

IPsec para OSPFv3 se puede configurar en una interfaz o en un área OSPFv3.

Para una mayor seguridad, debe configurar una política diferente en cada interfaz configurada con IPsec. Si se configuran IPsec para un área OSPFv3, la política se aplica a todas las interfaces de la zona, a excepción de las interfaces que tienen IPsec configurados directamente. Una vez IPsec está configurado para OSPFv3, IPsec es invisible para el usuario.

Para implementar el protocolo OSPFv3 en nuestra red WAN bancaria decidimos implementar cuatro áreas.

## 3.3 Diseño de la seguridad en la Red WAN-Bancaria.

La seguridad de la Red Bancaria está garantizada por dos aspectos uno lógico y otro físico:

- Utilización del estándar IPsec.
- Seguridad de acceso a los equipos de comunicación.

Dado que la información es uno de los activos más importantes de toda organización, y en una institución bancaria los niveles de seguridad de la información deben ser los más estrictos, junto a los procesos y sistemas que la manejan, deben ser protegidos convenientemente frente a amenazas que puedan poner en peligro la continuidad de los niveles de competitividad, rentabilidad y marco legal vigente.

Actualmente, la mayor parte de la información reside en equipos informáticos, redes de datos y soportes de almacenamiento, encuadrados todos dentro de lo que se conoce como sistemas de información. Estos

sistemas de información están sujetos a riesgos e inseguridades tanto desde dentro de la propia organización como desde fuera. A los riesgos físicos (accesos no autorizados a la información, catástrofes naturales, incendio, inundaciones, terremotos, vandalismo, etc.) hay que sumarle los riesgos lógicos (virus, ataques de denegación de servicio, etc.).

Las características de seguridad del IOS de Cisco para sus dispositivos de Red me permiten protegerme de los riesgos lógicos. IPsec es un componente obligatorio del protocolo IPv6 y es una funcionalidad del IOS de Cisco, me proporciona cifrado de datos de la red a nivel de IP y a todos los protocolos basados en IP como TCP y UDP.

Siendo IPsec un conjunto de estándares que integra funciones de seguridad basada en criptografía. Proporciona confidencialidad, integridad y autenticidad de datagramas IP.

OSPF para IPv6 me proporciona autenticación y protección con IPsec, en modo túnel IPsec me permite la encapsulación para proteger el trafico IPv6 unicat y multicast.

La interfaz de tunel virtual IPsec (VTI) ofrece protección criptográfica de sitio a sitio del trafico IPv6. El IPsec VTI permite que los routers IPv6 trabajen como gateways de seguridad, establecen túneles IPsec entre los routers de seguridad, y proporcionan protección criptográfica IPsec para el tráfico de las redes internas cuando se envía a través de la red IPv6. La figura 3.5 muestra el detalle del Túnel IPsec.

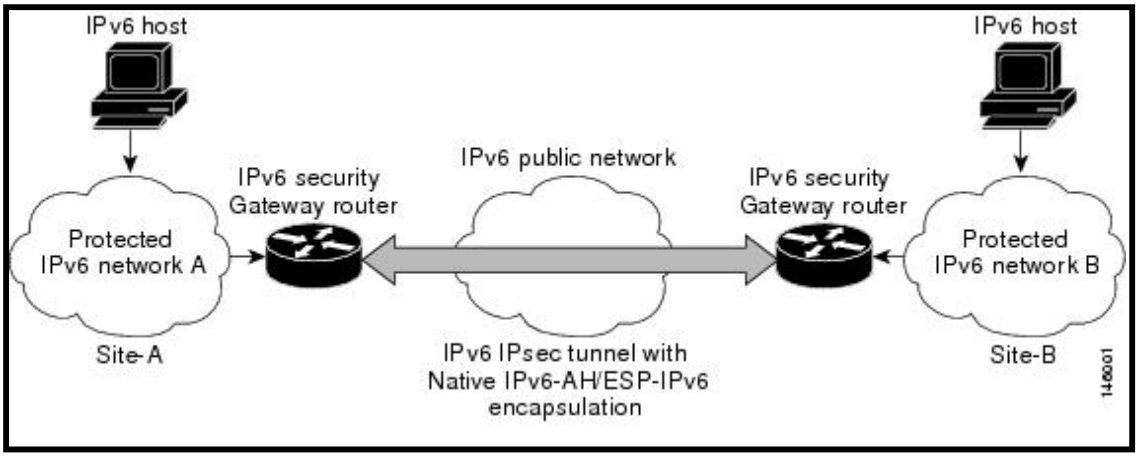



Figura 3.5 IPSec Tunnel Interface para IPV6 [30]

Seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Conviene aclarar que no siendo posible la certeza absoluta, el elemento de riesgo está siempre presente, independiente de las medidas que se tomen, por lo que se debe hablar de niveles de seguridad. La seguridad absoluta no es posible, la seguridad es un conjunto de

técnicas encaminadas a obtener altos niveles de seguridad en los sistemas informáticos.

Además, la seguridad informática precisa de un nivel organizativo, por lo que se dirá que:

SISTEMA DE SEGURIDAD = TECNOLOGIA + ORGANIZACIÓN

Para brindar seguridad a los equipos de comunicación, la institución bancaria solo permitirá acceder a los mismos de acuerdo a sus políticas de seguridad. Estas políticas de acceso son físicas directamente con los equipos y lógicas por cuanto se administran claves de acceso y solo tráfico de datos permitido por sus políticas.

La seguridad administrada por la institución Bancaria es especificada en 2 puntos:

- Seguridad de los enlaces, que no pueden acceder a la red equipos o personas no autorizadas, y las personas autorizadas a hacerlo sean de exclusiva confianza y con los conocimientos necesarios para hacerlo.

- Seguridad de los Servidores, teniendo acceso y las claves del mismo solo personal autorizado, además de filtros y firewall de protección levantados también en el servidor.

## 3.4 Selección de la Aplicación de Administración de red (NMS)

### 3.4.1 Análisis de la aplicación HP OpenView

[22] HP Open View es un conjunto de soluciones de software, amplio y modular para gerenciar y optimizar los servicios de TI e infraestructura de voz y datos.

Esta solución está compuesta de muchas partes que en un conjunto consideran todas las necesidades que un administrador de redes pueda tener. Dentro de los productos, se encuentran:

- Network Node Manager (NNM)
- Customer Views (CV)
- Services Information Portal (SIP)

Es de especial interés para el presente estudio el NNM, pues es el que se encarga de la administración de dispositivos SNMP, provee además capacidades para el descubrimiento de equipos y la posibilidad de mostrar graficas topológicas.

El NNM descubre todos los elementos a los que tiene acceso y los agrega a la topología, muestra además un sistema de alertas de los que tiene configurados. Dentro de la topología conforme se navega al segmento de red que se requiere observar, es posible tomar más acciones sobre los terminales, como observar alarmas específicas, monitorear interfaces, realizar conexiones telnet, entre otras aplicaciones. En la figura 3.6 se muestra la interface gráfica de software de monitoreo HP OpenView.

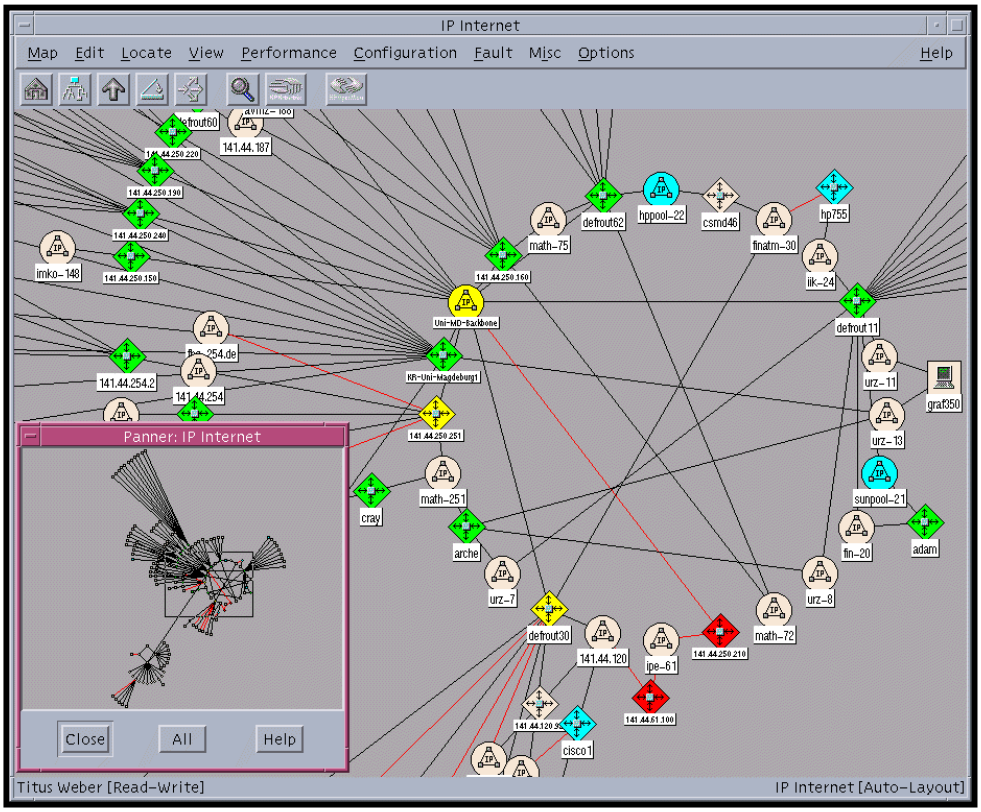



Figura 3.6 Interface gráfica de HP OpenView [22]

### 3.4.2 Análisis de la aplicación SolarWins

[31] Este sistema está basado en Web, a través de ICMP, SNMP, WMI y recolección de datos y comunicación Syslog me permite detectar, diagnosticar y resolver rápidamente problemas e interrupciones del rendimiento de red. El diagrama de monitoreo de SolarWinds se puede observar en la figura 3.7.

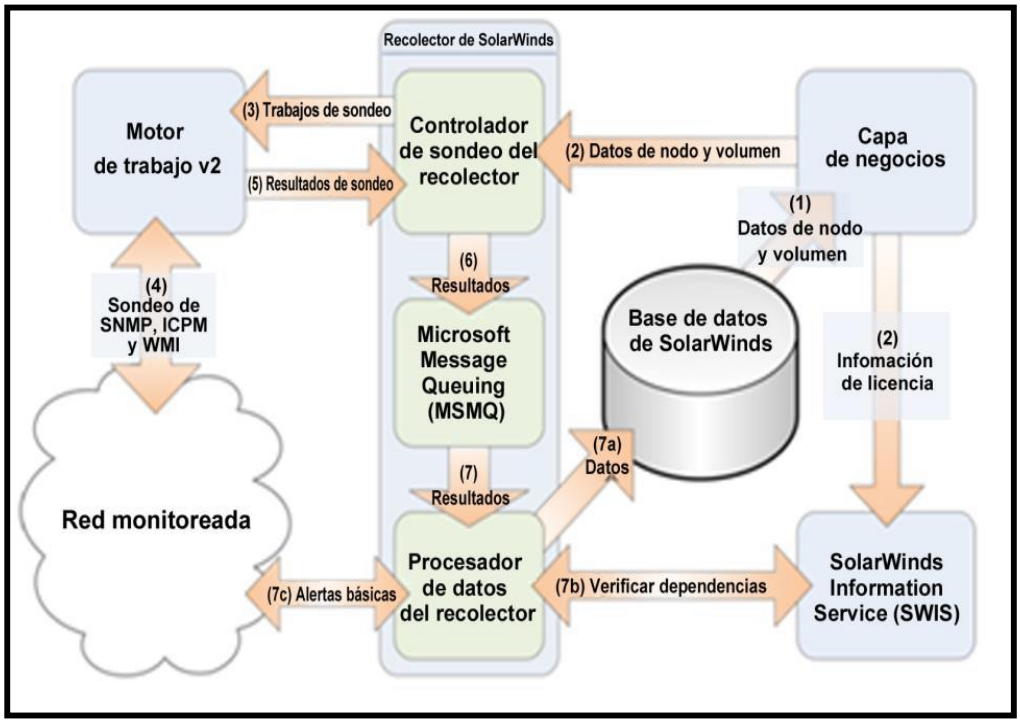



Figura 3.7 Diagrama de Monitoreo de SolarWinds [31]

Entras las características principales de SolarWinds:

Supervisa y analiza estadísticas de rendimiento de red detallada y en tiempo real, que permiten hacer un seguimiento visual y supervisar el rendimiento de la red de un vistazo. Además, el uso de dinámicas de mapas de topología de red y el descubrimiento de red automatizada, puede implementar y mantenerse al día con la evolución de su red.

Utiliza SNMP para analizar datos de enrutadores, conmutadores, servidores, etc. El sistema corre sobre Windows 2003 o 2008 Server.

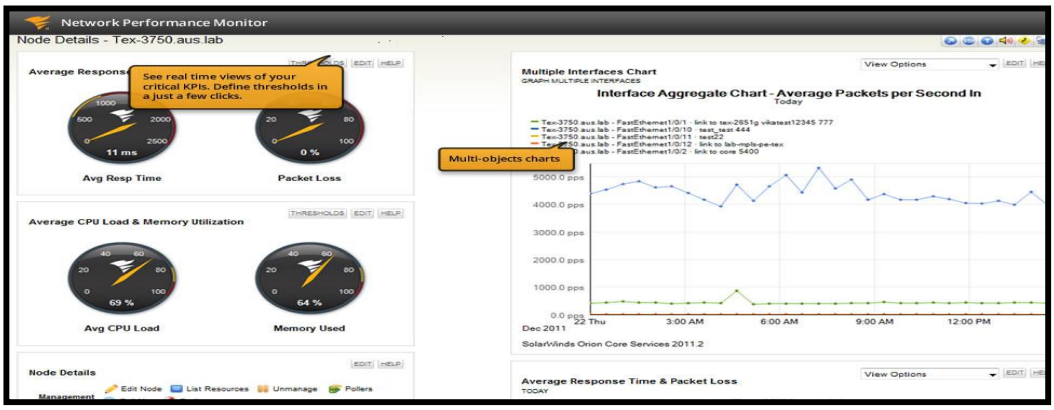



Figura 3.8 Interface Gráfica SolarWinds [22]

La figura 3.8 muestra interfaces para el monitoreo de un nodo, en esta se observa estadística de tiempo y respuesta. Promedio de paquetes por segundo, así como de utilización de memoria y CPU.

Las estadísticas son dadas en forma de instrumentos de medición para la última medición y como gráficos para observar datos históricos.

### 3.4.3 Análisis de la aplicación Nagios.

[32] Nagios es un sistema de código abierto de monitorización de equipos y servicios informáticos ampliamente utilizado, que vigila los equipos (hardware) y servicios (software) que se especifiquen, alertando cuando el comportamiento de los mismos no sea el deseado.

Posee una versatilidad para vigilar cualquier parámetro de interés de un sistema. Nagios envía alertas cuando un sistema deja de funcionar correctamente y permite su recuperación.

Características principales:

- Auto descubrimiento: Descubrirá automáticamente, creara el inventario y registrara las métricas de desempeño de sus servicios a través de la infraestructura física, virtual.

- Monitor: Desde métricas de desempeño hasta archivos de log, cambio de configuraciones a métricas de negocio. Se ejecuta en cualquier sistema operático.

- Alertas: Recibirá un aviso para prevenir la indisponibilidad de sus recursos, para que pueda ser proactivo en vez de reactivo.

- Diagnóstico y Motor de Gráficos: Se puede utilizar el sistema de gráficos y ejecutar un diagnostico en caliente en recursos remotos. Se puede ejecutar diagnósticos de sistema operativo, consultas, y ver el estado del servidor.

- Hecho a medida: Como software open source, está desarrollado para ser adaptado y configurado a sus necesidades. Una gráfica típica del nagios es como se muestra en la figura 3.9.

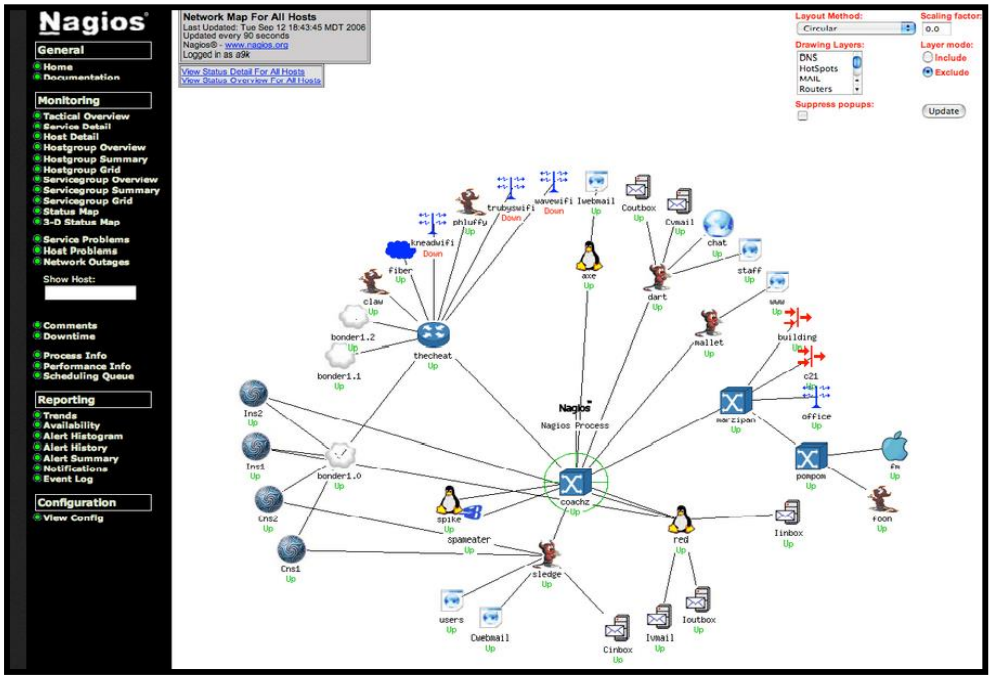



Figura 3.9 Interface Gráfica Nagios [32]

### 3.4.4 Análisis de la aplicación JFFNMS

[33] Las siglas JFFNMS corresponden a Just For Fun Network Management System. JFFNMS permite monitorizar dispositivos a través de la utilización del protocolo SNMP. La idea es definir una jerarquía de objetos interrelacionados a través de una serie de identificadores, y de unos procesos basados en el planificador del sistema que se ejecutan periódicamente y que tiene por objeto actualizar la información.

Así primero se identifica la red, a continuación los dispositivos que están conectados a ella. En el siguiente nivel las interfaces de cada dispositivo, es decir, todos aquellos elementos que pueden ser monitorizados dentro de un dispositivo, el adaptador de red, la memoria, el almacenamiento, etc.

El proceso consiste primero en definir y configurar los dispositivos a ser monitorizados y de qué manera. A partir de su OID y posición dentro de la MIB; en localizar los valores de las variables que representan estas interfaces y posteriormente vía el protocolo SNMP con las funciones *snmpget* o *snmpwalk*, recoger estos valores.

Una vez localizada la información, JFFNMS, permite representar la información, determinar el estado de los dispositivos, si están up o down, realizar graficas de rendimientos, mostrar alarmas cuando se alcanzan ciertos umbrales, generar SLA's de dispositivos e informes.

Las características principales son:

- JFFNMS es un sistema de gestión y monitorización de red diseñada para monitorizar una red IP.
- Es un proyecto desarrollado por Javier Szyszlican.
- Se encuentra en constante desarrollo.
- Se trata de software libre y está bajo licencia GPL.
- Permite monitorizar una red IP mediante SNMP, Syslog y Tacacs+
- Puede ser utilizado para monitorizar cualquier dispositivo SNMP, servidor, enrutador, puerto TCP o cualquier elemento que se desee siempre que se programe una extensión adecuada a dicho elemento para JFFNMS.
- También dispone de características orientadas al manejo de dispositivos Cisco.
- JFFNMS está descrito en PHP y funciona en eventos GNU/Linux, FreeBSD y Windows.

- JFFNMS genera gráficas para todos los dispositivos de la red tráfico de red, utilización de CPU, errores, etc.
- Tiene soporte de base de datos (MySQL), integra logs de Syslog y autenticación e informes de Tacacs+.
- JFFNMS se basa en las tecnologías: Apache, MySQL, PHP, RDDTool y SNMP.

En la figura 3.10 se observa el análisis que realiza el software JFFNMS.

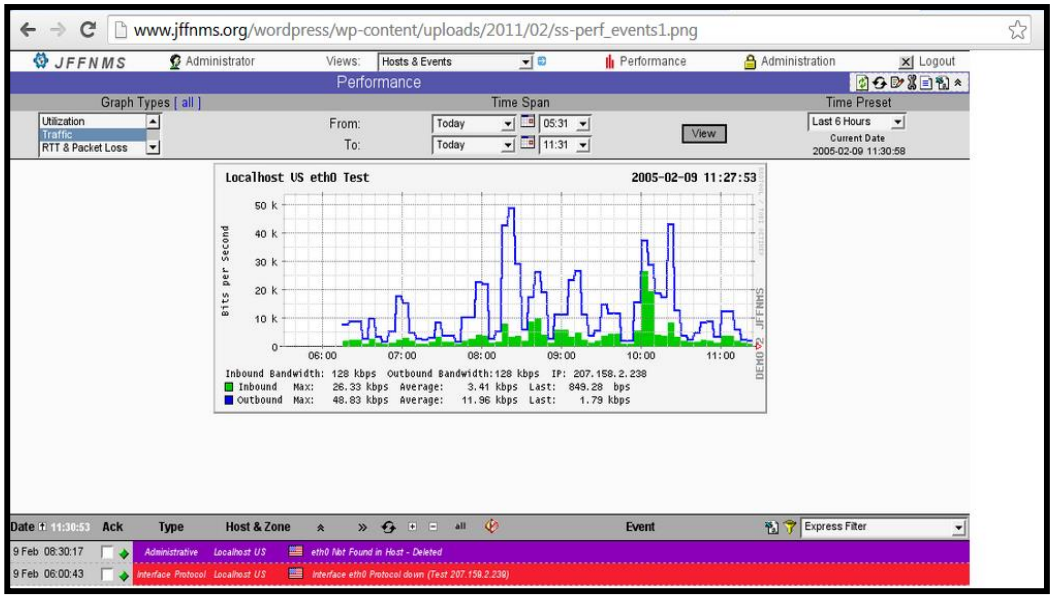



Figura 3.10 Interface Gráfica JFFNMS [33]

# CAPÍTULO 4

## 4 IMPLEMENTACIÓN Y SIMULACIÓN

### 4.1 Configuración de enrutador de Red Cisco

Para realizar la simulación de nuestra red de estudio utilizamos el software de simulación grafica de redes de datos GSN3, el cual me permite implementar el diseño en diferentes topologías. GNS3 soporta el, IOS de los enrutadores CISCO, ASA firewall, Switches y Pix firewall.

GNS3 está basado en Dynamips, PEMU (incluyendo el encapsulador) y Dynagen, desarrollado en Phyton, utiliza la tecnología SVG (gráficos vectoriales escalables) para proveer símbolos de alta calidad para el diseño de las topologías de red.

**Dynamips** es un emulador de encaminadores Cisco, emula a las plataformas 1700, 2600, 3600, 3700 y 7200 y ejecuta imágenes IOS.

**Dynagen** permite a los usuarios listar los dispositivos, suspender y recargar instancias, determinar y administrar los valores de idle-pc, realizar capturas.

La tabla 4.1 detalla las ventajas y desventajas del uso de GNS3.

Tabla 4.1 Ventajas y Desventajas de GNS3

| Ventajas | Desventajas |
|---|---|
| Fácil de Usar | Al emular más de 3 enrutadores en un solo computador esta no responde. |
| Fácil instalación | Para su correcto funcionamiento requiere un computador o computadores con altos recursos. |
| Gratuito | |
| Trabajo con sistemas IOS reales | |
| Apropiado para simular grandes redes, ya que me permite que un cliente GNS3 pueda correr en una maquina diferente al que contiene el emulador repartiendo el procedimiento entre varios PCs. | |

El esquema siguiente nos permite crear una Red WAN sobre el protocolo IPv6 hacia nuestro Servidor NMS, para el efecto se utilizó enrutadores simulados Cisco de la familia 7200.

Este esquema se lo realizó mediante el uso del simulador GNS3 y el IOS 15.0 que ya posee soporte para IPv6. En la figura 4.1 se describe el esquema de Red WAN que fue implementado en GNS3.

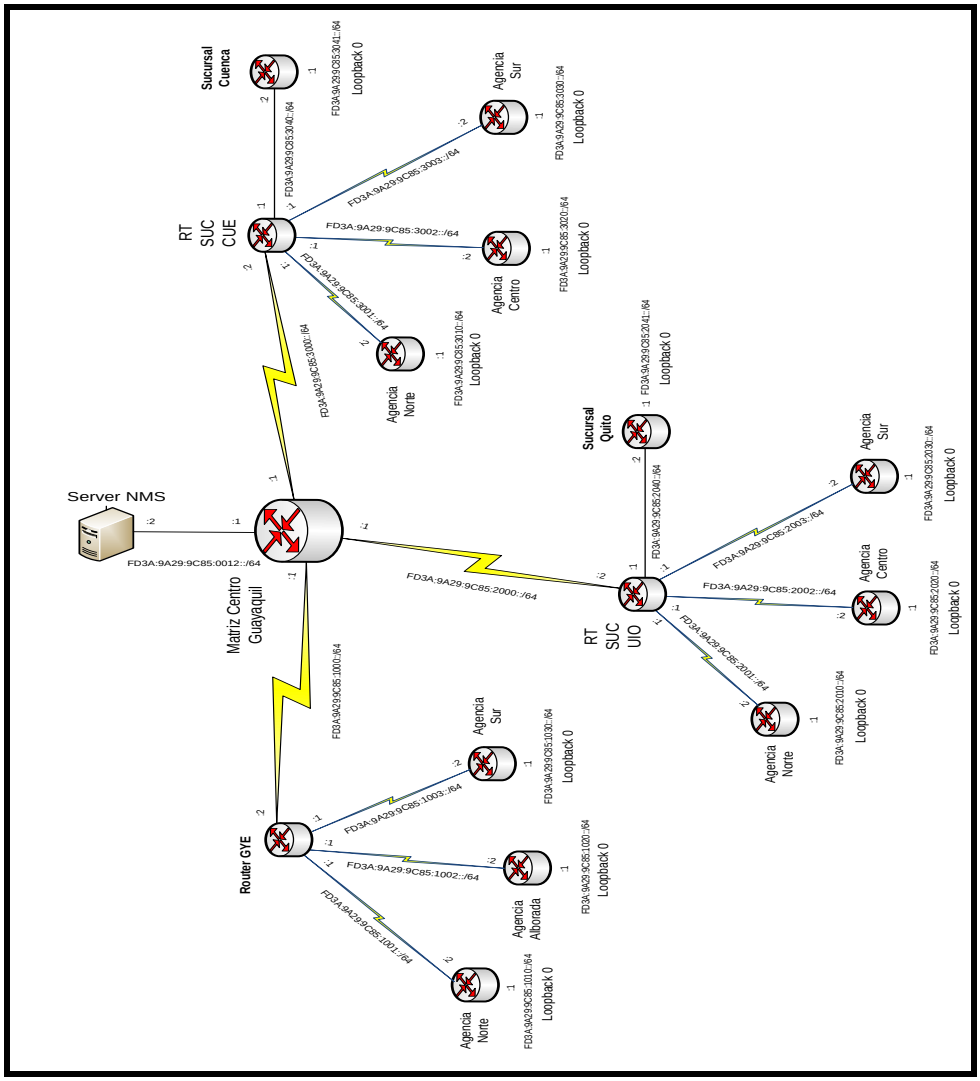



Figura 4.1 Esquema de Red WAN

EL enrutador **Matriz-Centro-Guayaquil**, es el enrutador principal el cual nos permite la comunicación hacia nuestras distintas agencias. Habilitamos los siguientes comandos IPv6 en cada uno de los enrutadores, con el cual habilitamos el protocolo IPv6. Los comandos que

habilitan el protocolo IPv6 en los enrutadores cisco se detallan en la Tabla 4.2.

Tabla 4.2 Comandos de Habilitación IPv6

| | |
|---|---|
| #ipv6 unicast-routing | Habilita el reenvío de paquetes de datos unicast. |
| #ipv6 cef | CEF (Cisco Express Forwarding) es un feature avanzado de Cisco IOS que permita un modo de conmutación más rápido en los dispositivos Cisco. |
| #ipv6 enable | Configura automáticamente una dirección local de enlace IPv6 en la interfaz, y habilita la interfaz para el procesamiento de IPv6.<br>La dirección local de vínculo sólo se puede utilizar para comunicarse con nodos en el mismo vínculo. |

Configuramos las interfaces y definimos que la red de área local de la interface FastEthernet 2/0 que nos da acceso al Servidor NMS pertenece a la subred FD3A:9A29:9C85:12:: / 64.

Las diferentes direcciones son configuradas en las interfaces del enrutador, las direcciones son del tipo ULA direcciones privadas IPv6, direcciones que no serán publicadas en internet. Las direcciones IPv6 asignadas a cada interface del enrutador principal se detallan en la tabla 4.3.

Tabla 4.3 Direcciones IPv6 Enrutador Principal.

| Interface | Dirección IPv6 |
|---|---|
| FastEthernet 2/0 | FD3A:9A29:9C85:12::1/64 |
| Serial 1/0 | FD3A:9A29:9C85:1000::1/64 |
| Serial 1/1 | FD3A:9A29:9C85:2000::1/64 |
| Serial 1/2 | FD3A:9A29:9C85:3000::1/64 |

No se asigna direcciones IPv4 a ninguna interface para garantizar que todos los paquetes que se intercambien entre las redes utilicen IPv6 como protocolo de red. El protocolo de encapsulamiento en la red WAN es HDLC.

Se muestra como ejemplo en la Figura 4.2 el protocolo que está habilitado en las interfaces del enrutador principal, los demás enrutadores que simulan mi red WAN tienen igual configuración con sus respectivas direcciones IPv6.

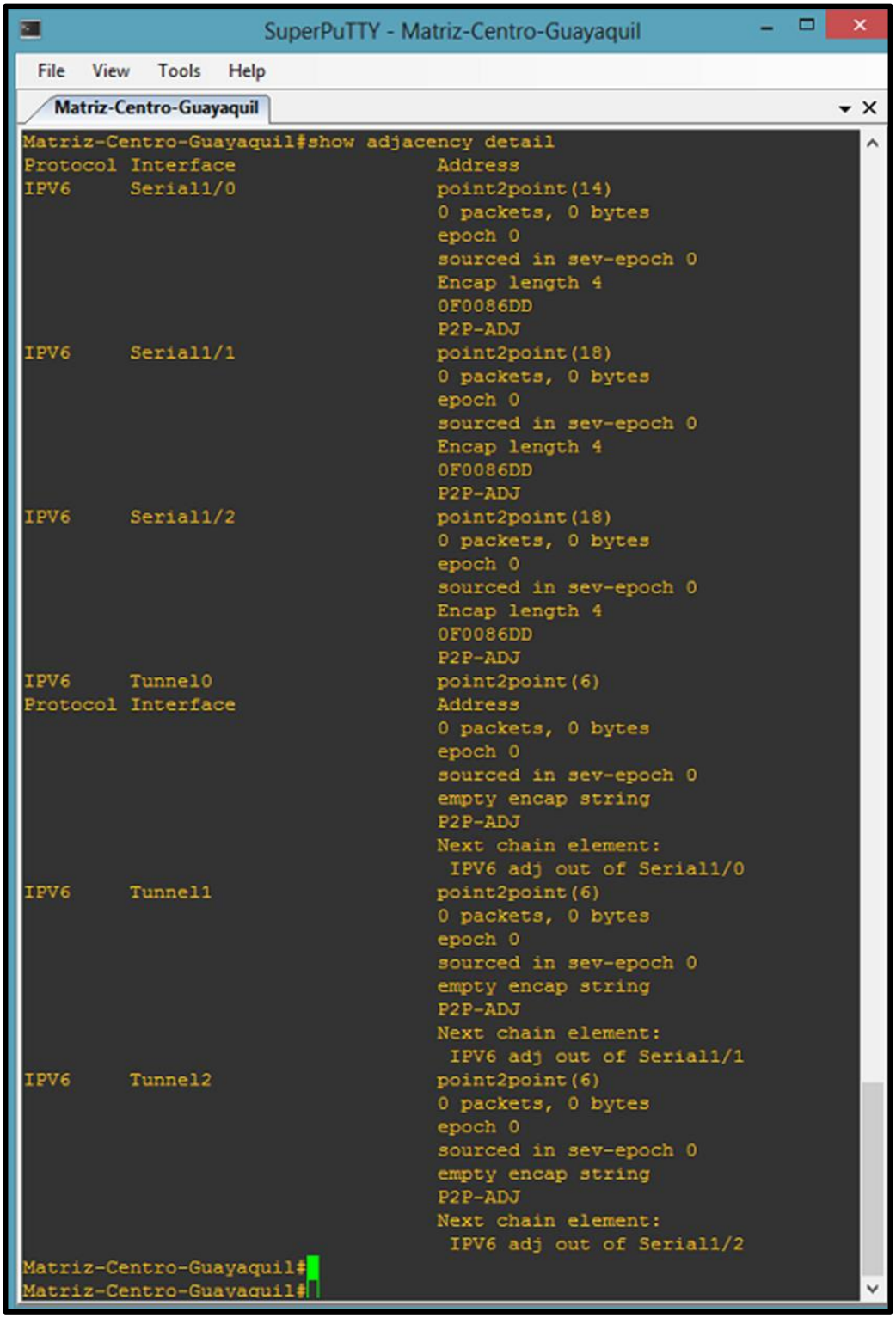



Figura 4.2 Detalle de Protocolos Activos

## PROTOCOLO DE ENRUTAMIENTO OSPFv3

El protocolo de enrutamiento que utilizamos es la versión 3 del protocolo OSPF. La figura 4.3 detalla los parámetros de operación del Protocolo OSPFv3 en nuestra Red WAN.

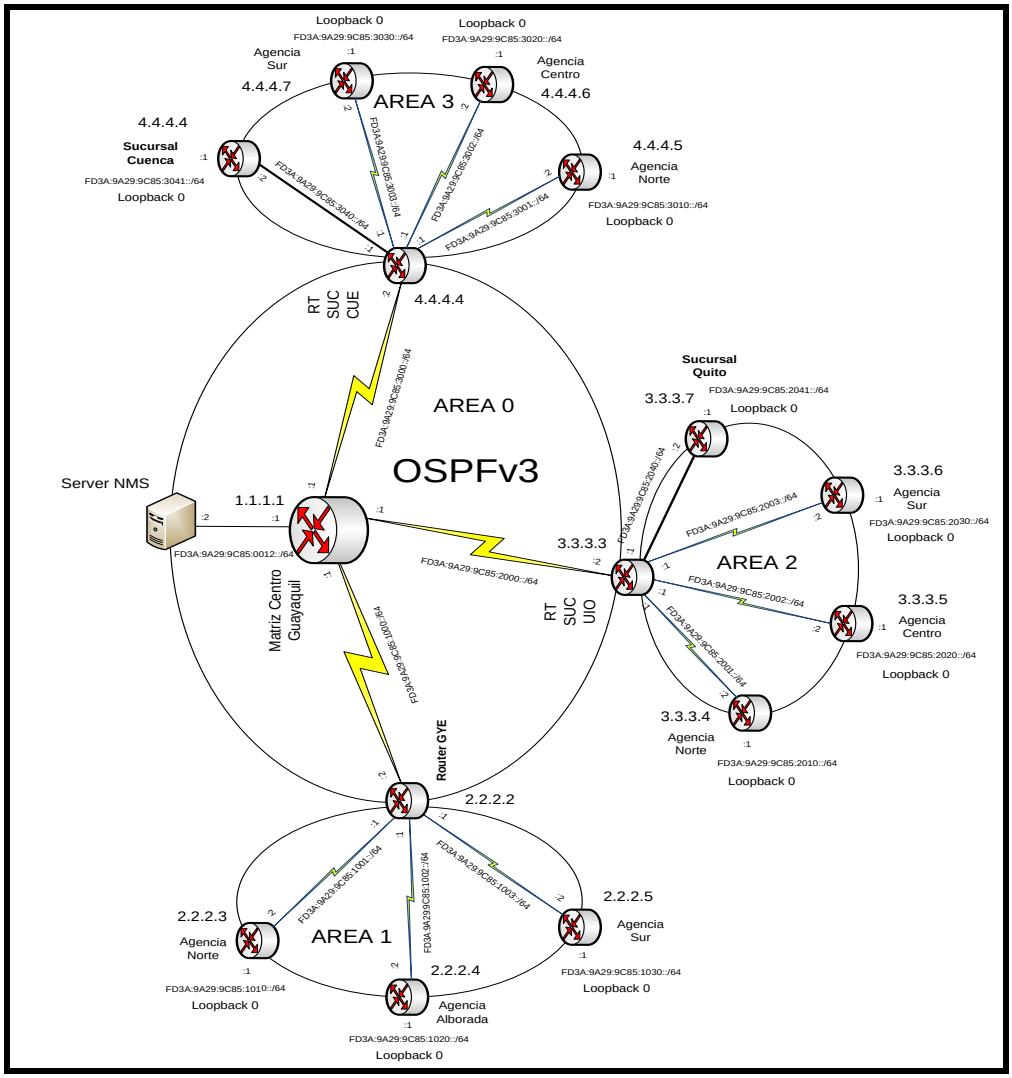



Figura 4.3 Protocolo de Enrutamiento OSPFv3

Para habilitar el proceso de enrutamiento OSPFv3 en cada una de las interfaces aplicamos los siguientes comandos que se detallan en la Tabla 4.4.

Tabla 4.4 Comandos de Habilitación de Proceso OSPF3

| | |
|---|---|
| Router(config)# ipv6 ospf 1 área 0 | Configura un área en OSPFv3 |
| Router(config)# ipv6 router ospf 1 | Entra en el modo de configuración del router y crea un proceso de enrutamiento IPv6 OSPF |
| Router(config-router)# router-id 1.1.1.1 | Permite el uso de un ID fijo en el router. |

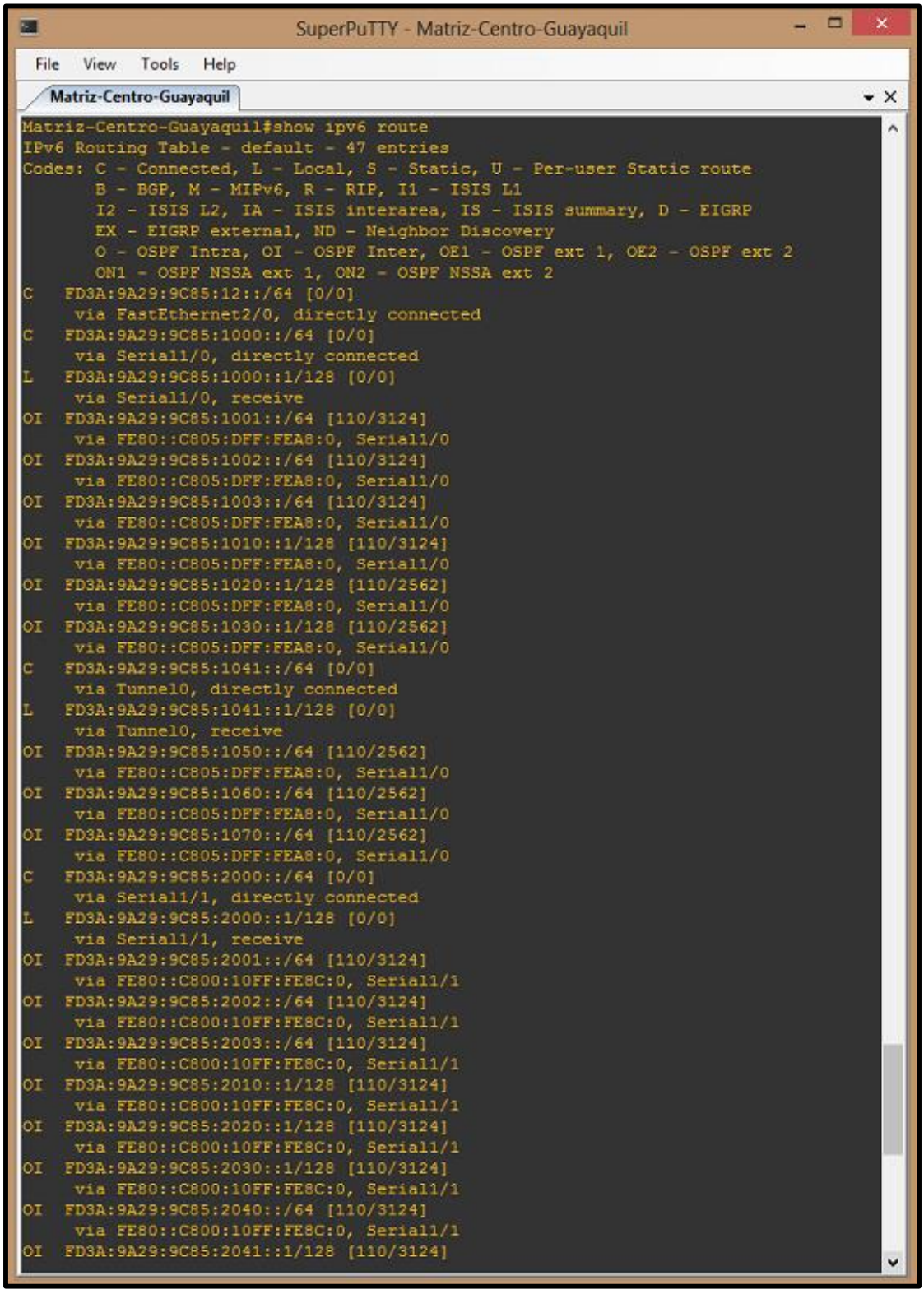
Definimos la tabla de ruta estática, utilizamos la ruta por defecto para que todo paquete que no conocemos el destino sea enviado por la interface fastethernet hacia el servidor de monitoreo NMS.

# ipv6 route ::/0 Fastethernet 2/0

En la figura 4.4 se observa las direcciones de Red aprendidas por el enrutador principal, permitirá la interconexión WAN, desde el servidor de

monitoreo NMS hacia los enrutadores y desde los enrutadores hacia el servidor de monitoreo NMS.

Tabla de rutas obtenidas mediante el proceso OSPFv3.



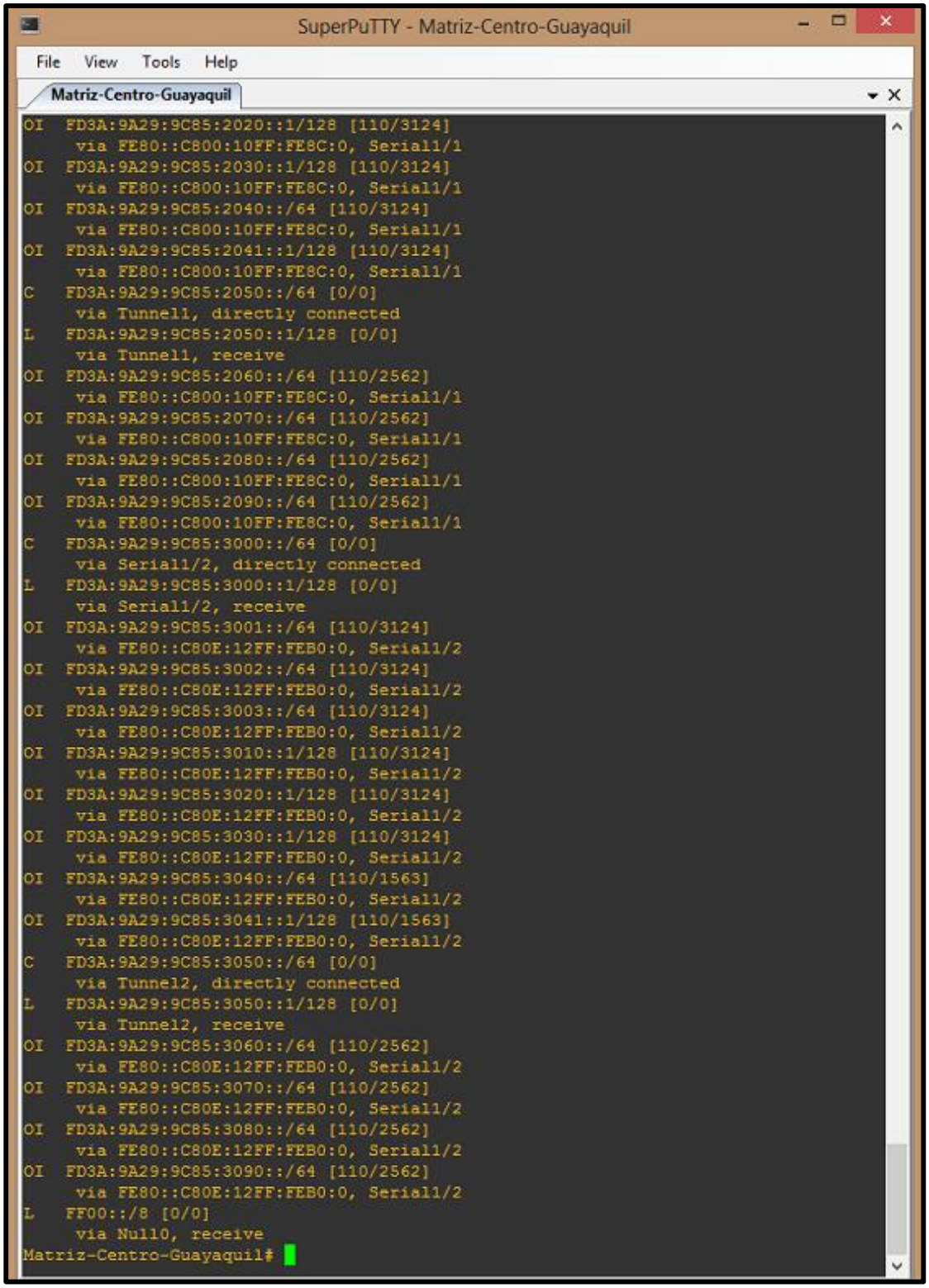



Figura 4.4 Segmentos de Red IPv6 obtenidas en proceso OSPFv3

## IMPLEMENTACIÓN IPSEC Y TUNNEL

Los parámetros de configuración de cada uno de los enrutadores que forman nuestra red WAN son iguales a la de mi enrutador principal, el cambio radica en las direcciones IPv6 que serán habilitadas en función de mi esquema de direccionamiento tal como se detalló en la sección 3.2.2.1

El esquema de implementación de IPsec se detalla en las figuras 4.5 y 4.6 donde se simula el establecimiento de los túneles y los parámetros de seguridad requeridos en el protocolo IPsec.

El detalle de los comandos de configuración del enrutador principal se puede observar en el anexo A.

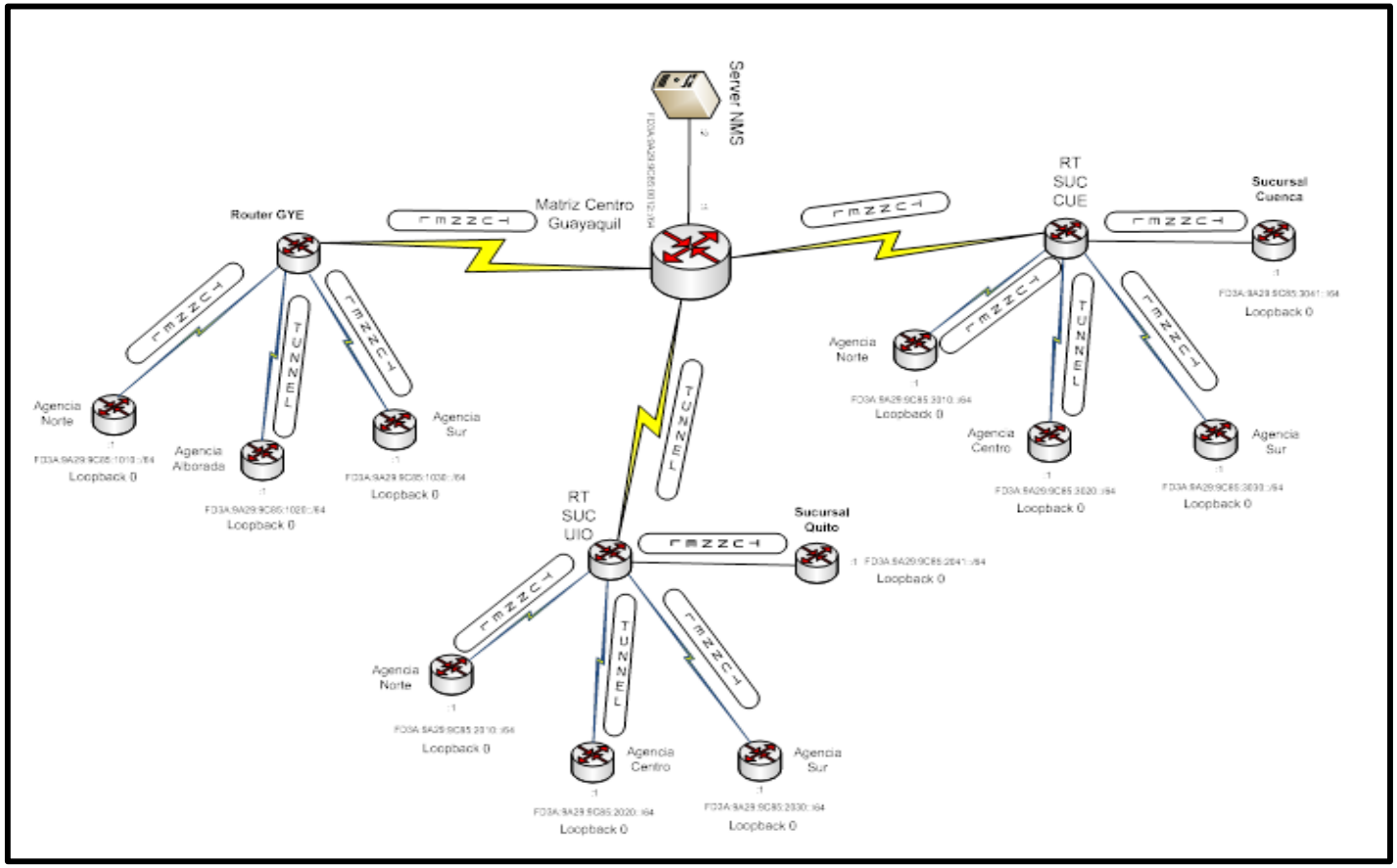



Figura 4.5 Esquema del Protocolo IPsec y Tunnel

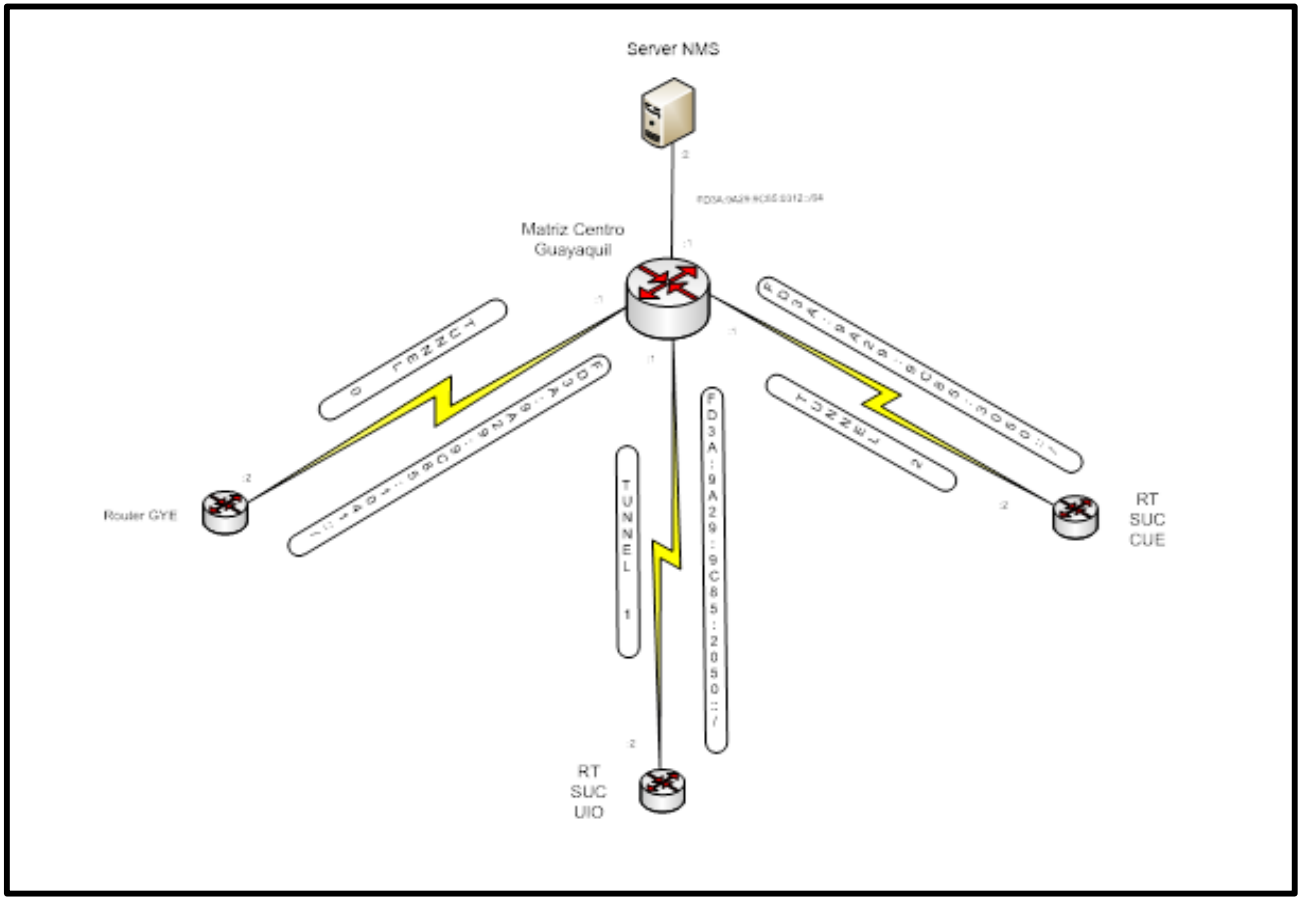



Figura 4.6 Esquema de Tunnel IPv6

Los protocolos Criptográficos activos y la política Criptográfica activa, en nuestro enrutador Principal se detallan respectivamente en la figura 4.7 y 4.8.

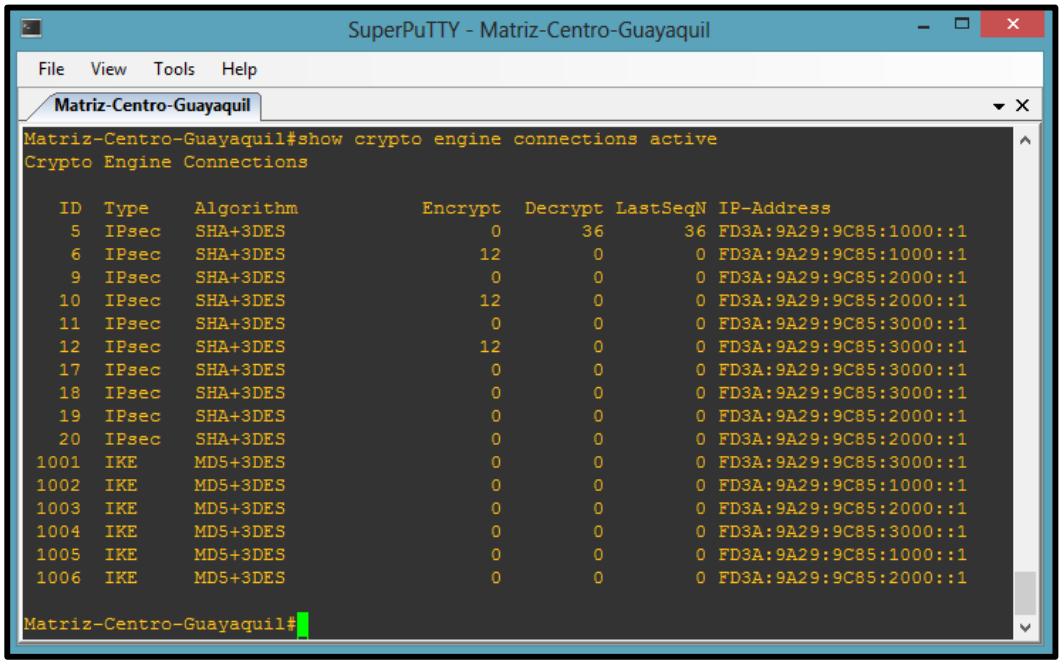



Figura 4.7 Protocolos Criptográficos Activos

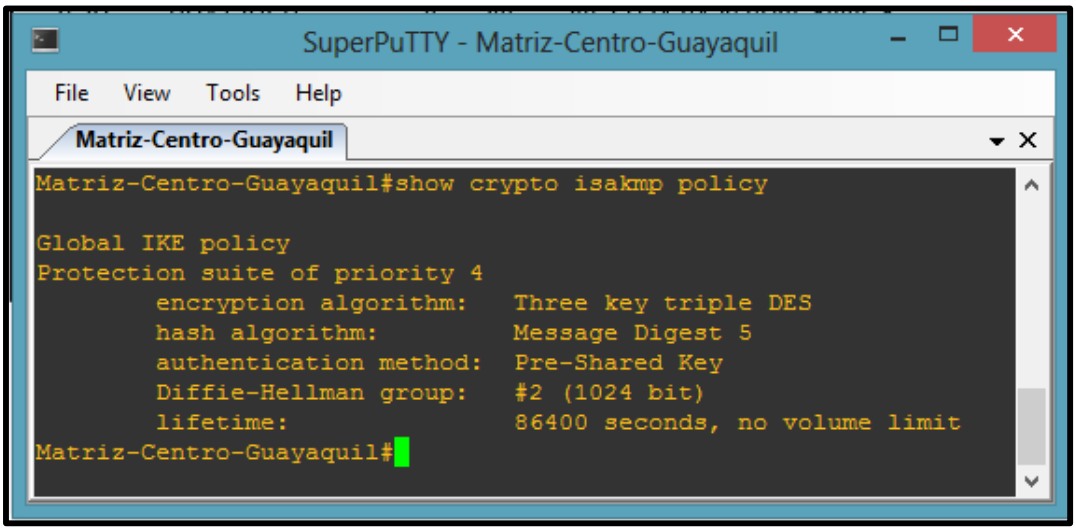



Figura 4.8 Política Criptográfica

Los túneles activos en nuestro enrutador Principal se pueden obtener mediante el comando Show crypto sessión y los resultados obtenidos se detallan en la figura 4.9.

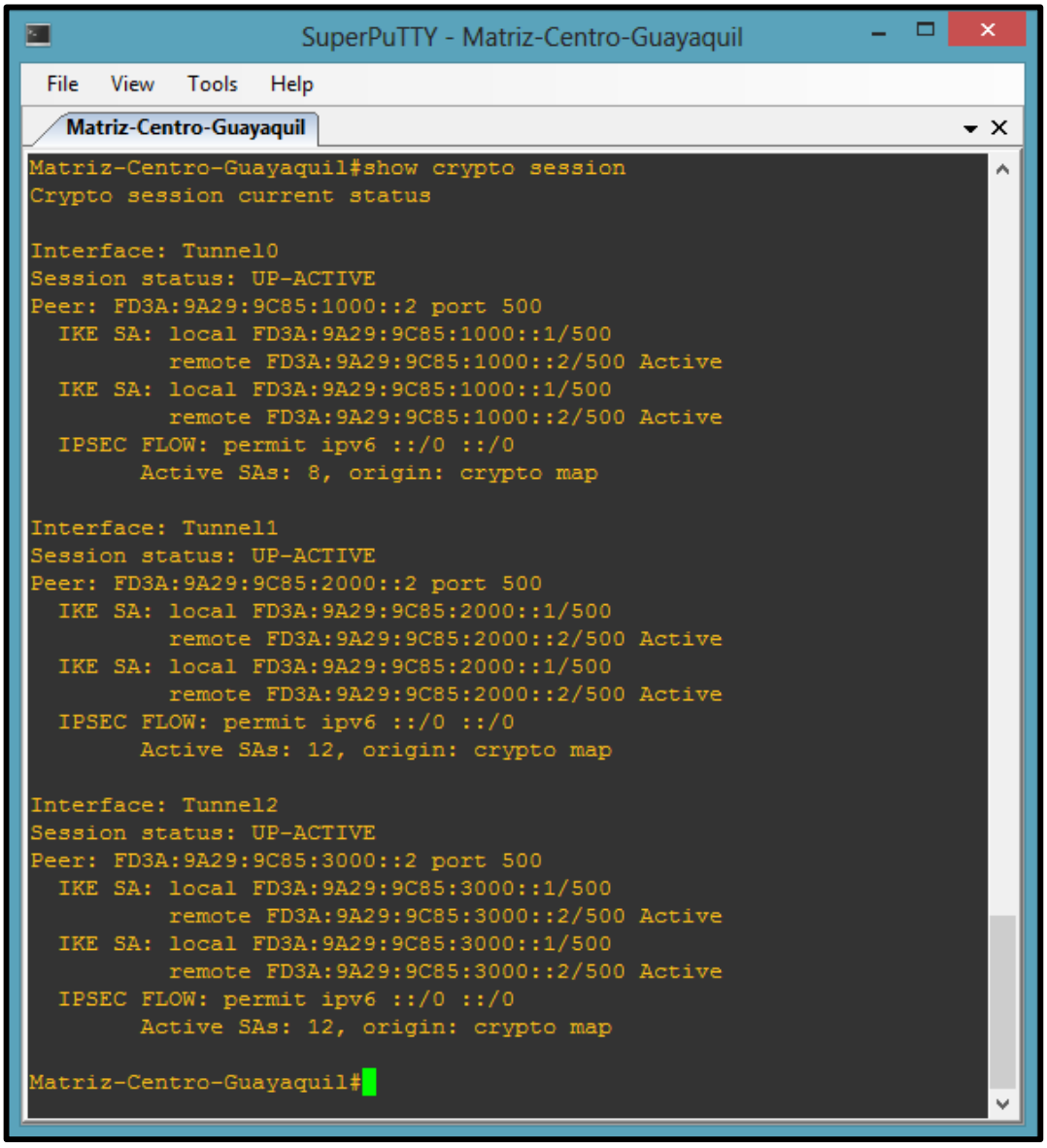



Figura 4.9 Estado de Túneles Criptográficos

## 4.2 Configuración del Servidor de Administración de la Red (NMS).

### 4.2.1 Instalación del sistema operativo de código libre (Open Source).

El servidor de monitoreo NMS inicialmente planificado para la realización de esta tesina, seria implementado en Nagios XI. La implementación de Nagios XI se realiza bajo el sistema operativo de código libre Centos.

Luego de realizar la instalación de Nagios XI en un servidor físico, que sería nuestro Servidor NMS de monitoreo de red, se inició el Auto-Discovery hacia nuestro enrutador principal de nuestra red WAN implementado en otra máquina física, cuya dirección IPv6 es FD3A:9A29:9C85:12::1, como se muestra en la gráfica 4.10.

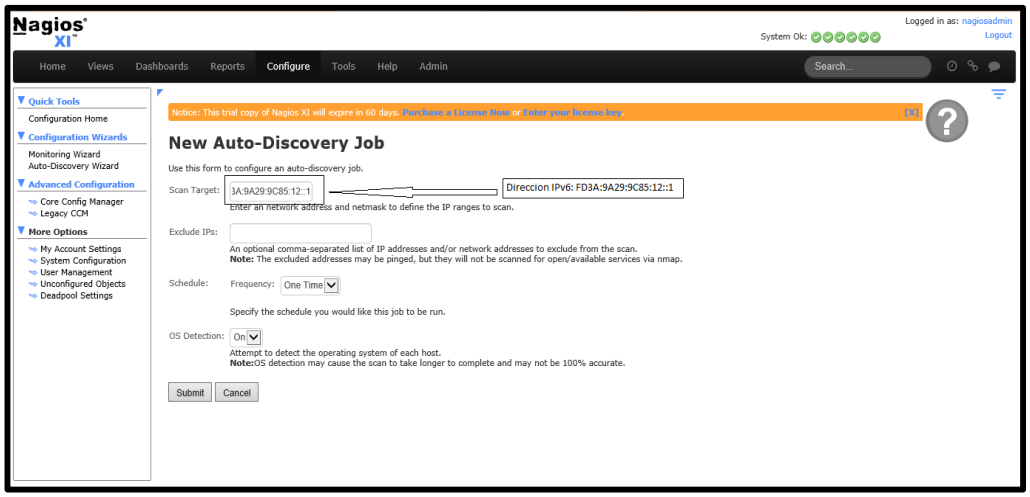



Figura 4.10 Auto Descubrimiento de Red.

Luego de realizar el Auto-Discovery nos muestra el servidor NagiosXI que el formato de caracteres ingresados no es admitido. Como se detalla en la figura 4.11.

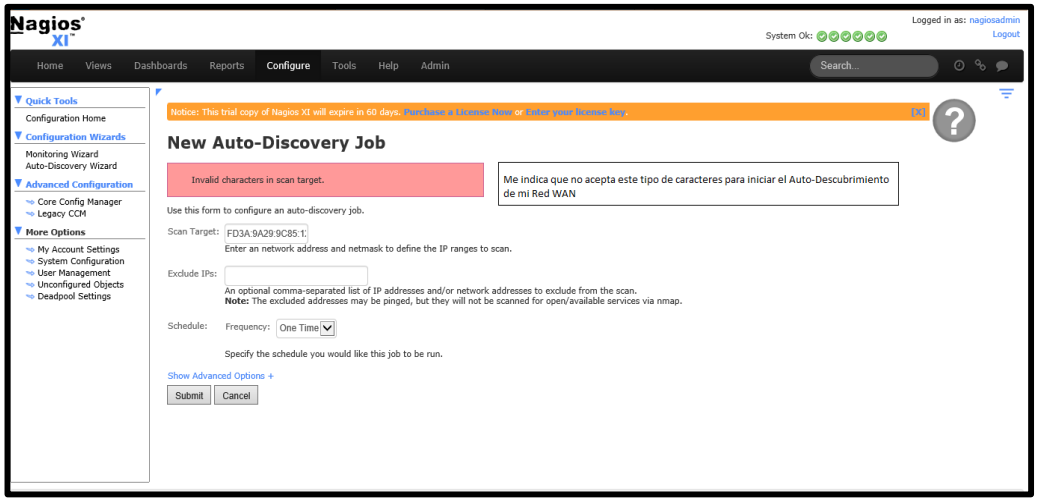



Figura 4.11 Mensaje de error de Ingreso de caracteres

Se debe ingresar direcciones en el formato IPv4 como se muestra en la figura 4.12.

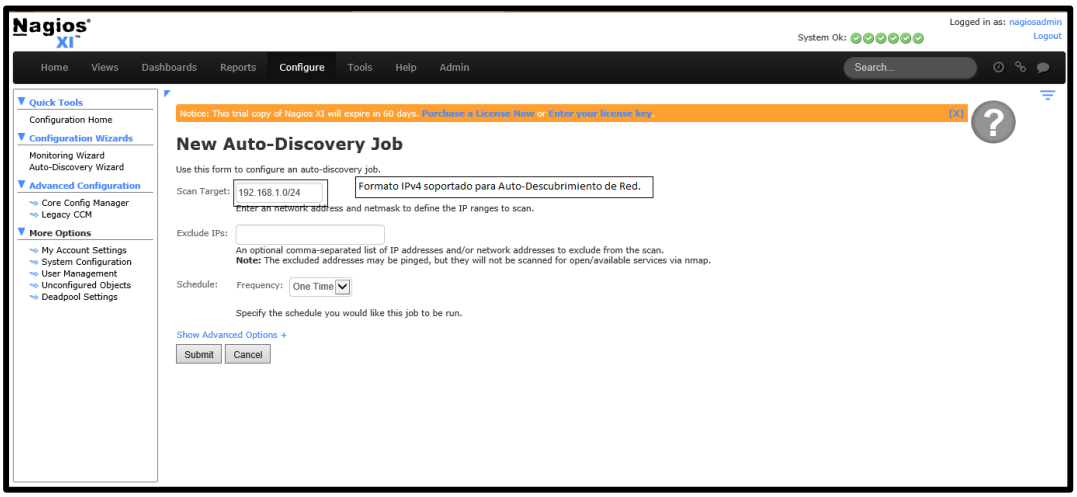



Figura 4.12 Caracteres permitidos en Auto Descubrimiento

### 4.2.2 Instalación de aplicación de Administración de Red (NMS software).

Network Performance Monitor, es una aplicación de Solarwinds que permite una simple detección de mi red, posee entre sus características.

- Supervisa enrutadores, conmutadores, servidores y cualquier otro dispositivo que tenga habilitado SNMPv1, SNMPv2c y SNMPv3.

- Supervisa enrutadores, conmutadores virtualizados igual que los físicos.
- Realiza el monitoreo en dual stack es decir IPv4 o Ipv6.
- Recoge datos sobre el estado y el rendimiento de la red, incluidos ICMP, SNMP y Syslog.
- Permite una integración abierta de Microsoft®SQL y MIB.
- Posee herramientas para generar y manejar traps.

Por esta razón se decidió usar esta aplicación, qué me permite gestionar mis enrutadores virtuales creados en GNS3, implementados con direccionamiento IPv6 y ser gestionados con SNMPv3.

La aplicación Network Performance Monitor, se puede descargar un demo con valides de 30 días en http://www.solarwinds.com/network-performance-monitor.aspx.

La instalación en muy sencilla solo tendría que aceptar los requerimientos de licencia y usuario temporal. Una vez instalado se inicia el centro de descubrimiento automático donde se ingresa la versión de SNMP y la comunidad. La figura 4.13 muestra la pantalla de Auto Descubrimiento.

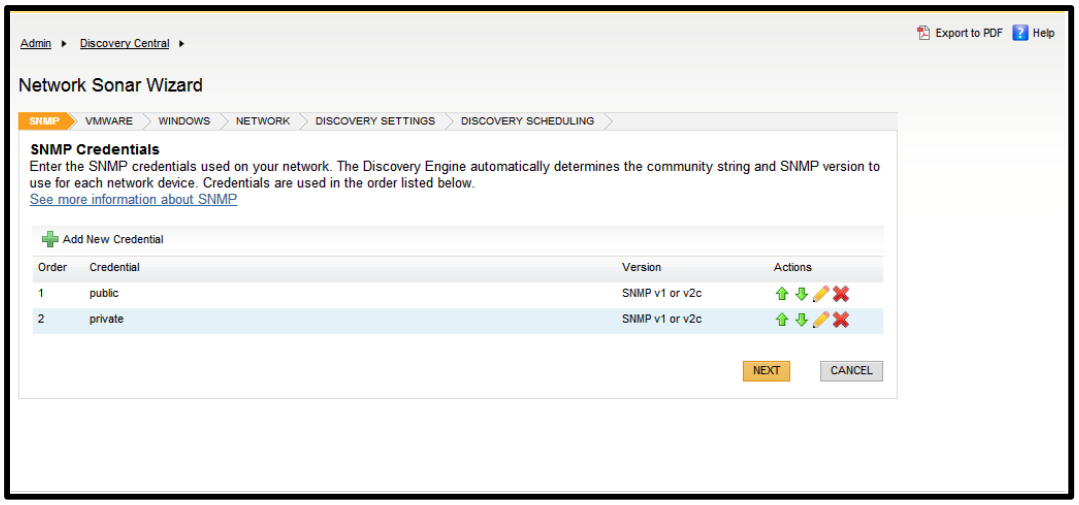



Figura 4.13 Pantalla de Auto Descubrimiento

Para iniciar el monitoreo se procede a ingresar el nombre de la comunidad que deseamos gestionar y la versión del protocolo SNMP. En la figura 4.14 se detalla el ingreso de Comunidad que será gestionada.


Figura 4.14 Ingreso de Comunidad SNMPv1 o SNMPv2

En la figura 4.15 se configuran los parámetros de la versión SNMPv3, se ingresa el nombre de usuario y los protocolos de autenticación y encriptación junto con las claves asignados.

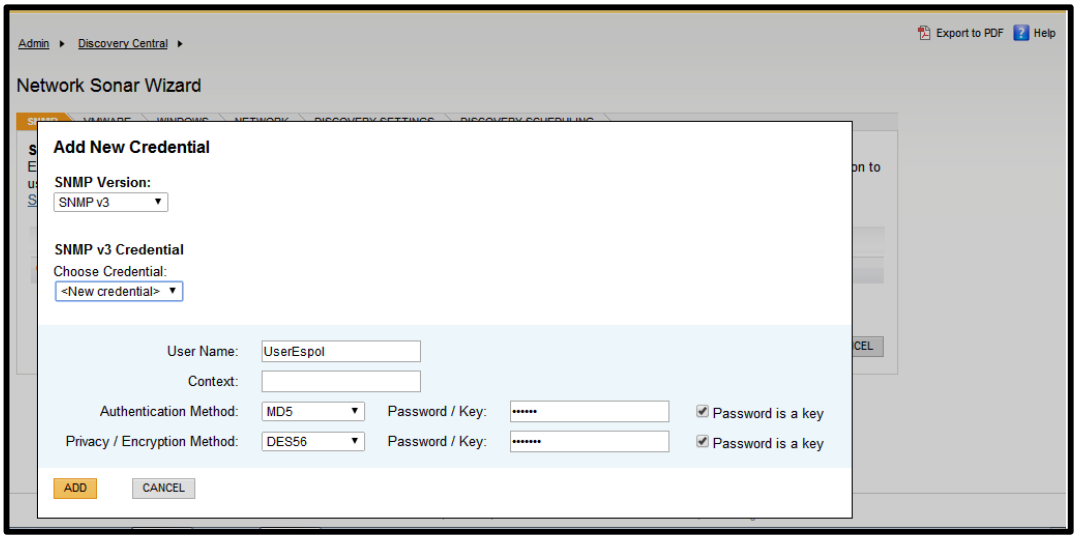



Figura 4.15 Ingreso de Credenciales SNMPv3

Network Performance Monitor, posee por defecto la posibilidad de descubrir direcciones IPv6 tal como se observa en la figura 4.16.

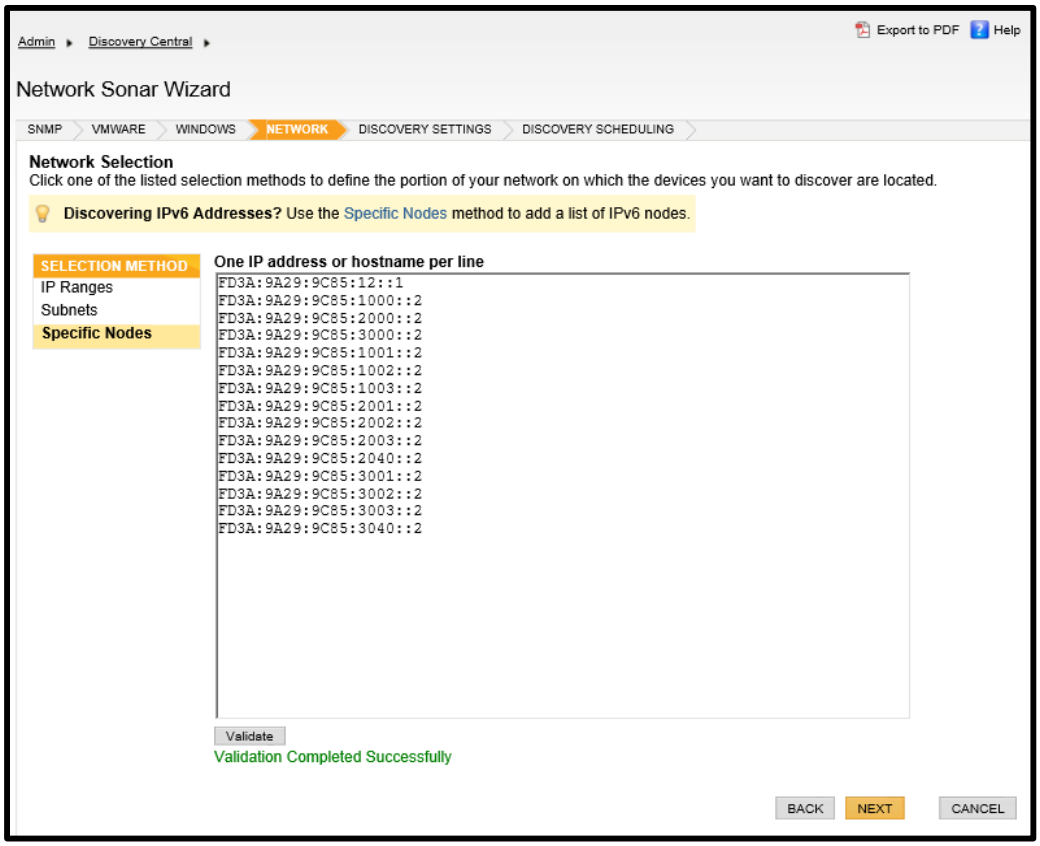



Figura 4.16 Ingreso de Direcciones IPv6

Luego del descubrimiento de mi red WAN los resultados que se observan son los que se muestran en la Figura 4.17. Se aprecia marca de enrutador, nombre, modelo, protocolo de gestión, tipo de interfaces y encapsulamiento.

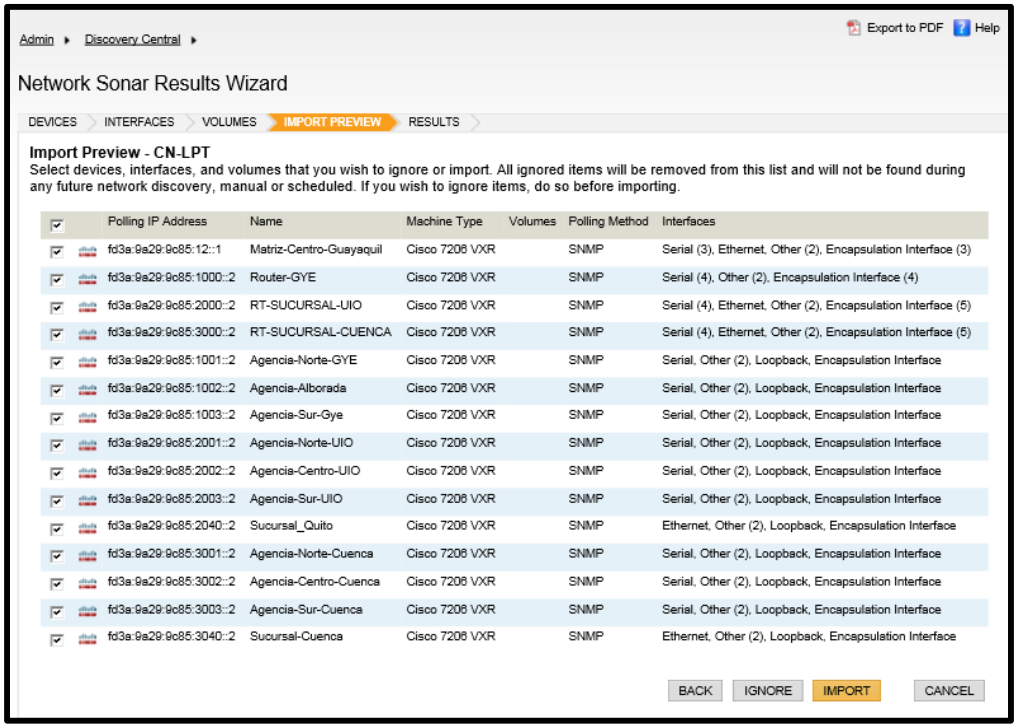



Figura 4.17 Resultado de Exploración

El detalle del protocolo SNMP en sus diversas versiones se detallara en la sección 4.4.

## 4.3 Configuración de Agentes en los elementos de Red (Management Element).

Los equipos que serán monitoreados y gestionados serán los enrutadores Cisco y serán a los que debemos habilitar los elementos de Monitoreo de Red. La figura 4.18 muestra el esquema de transmisión de los mensajes SNMP.

CONFIGURACIÓN SNMP

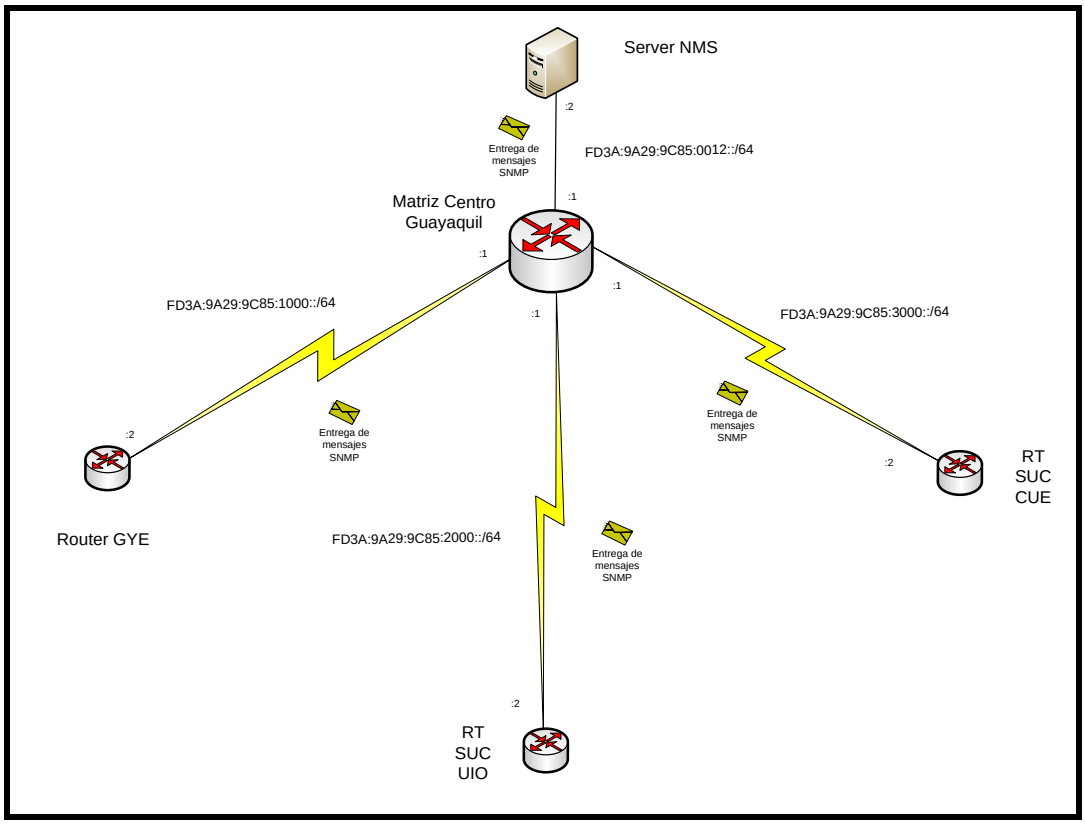



Figura 4.18 Esquema de Transmisión de mensajes SNMP

Los comandos siguientes nos permiten crear la comunidad snmp que llamare Tesis_Espol y asignare la dirección IPv6 de nuestro servidor NMS con la versión snmp que se asignó a nuestra comunidad.

#snmp-server community Tesis_Espol

#snmp-server host FD3A:9A29:9C85:0012::2/64 version 1 Tesis_Espol

#snmp-server host FD3A:9A29:9C85:0012::2/64 version 2c Tesis_Espol

En la versión SNMPv3 necesitamos configurar grupos y usuarios con protocolos de autenticación y niveles de seguridad, para lo cual utilizamos los siguientes comandos.

Ingresamos a los enrutadores e ingresamos en modo privilegiado.

#snmp-server group **GrupoEspol** v3 priv read **ReadEspol** write **WriteEspol**

#snmp-server user **UserEspol GrupoEspol** v3 auth md5 **kwnxpd** priv des **1971kwn**

#snmp-server view **ReadEspol** iso included

#snmp-server view **WriteEspol** iso included

#snmp-server host **FD3A:9A29:9C85:0012::2** version 3 priv UserEspol

#snmp-server host enable traps

- Views especifico los OIDs que van a poder ser accedidos para escritura o lectura por los usuarios de un grupo específico de SNMPv3.

- Group SNMPv3 que especifica el nivel de seguridad que se va a utilizar y al cual se le asignan las vistas que creamos anteriormente para permitir o restringir el acceso a ciertos MIBs/OIDs.

- User de SNMPv3 especificamos el nivel de seguridad y el protocolo para la autenticación.

En el anexo A detallo el estado del enrutador Matriz-Centro-Guayaquil, los demás enrutadores que conforman mi red WAN tienen igual característica con sus respectivas direcciones IPv6 asignadas en el esquema de direccionamiento IPv6.

## 4.4 Uso de Analizador de paquetes para revisar el tráfico de la Red.

El analizador de protocolos que utilizaremos para capturar el tráfico de nuestra red WAN en el Wireshark se basa en el uso de las librerías Pcap soporta el análisis de una gran cantidad de protocolos entre ellos la nueva

versión del protocolo de internet IPv6 y los protocolos de gestión SNMPv1, SNMPv2c y SNMPv3.

Para descargar el programa nos dirigimos a la página http://www.wireshark.org/download.html su instalación es bastante sencilla. Se necesita instalar los requisitos de licencia y librerías adicionales para dejar operativo nuestro software de análisis de protocolos. Las opciones de captura de tramas con el uso de Wireshark se pueden observar en la figura 4.19.

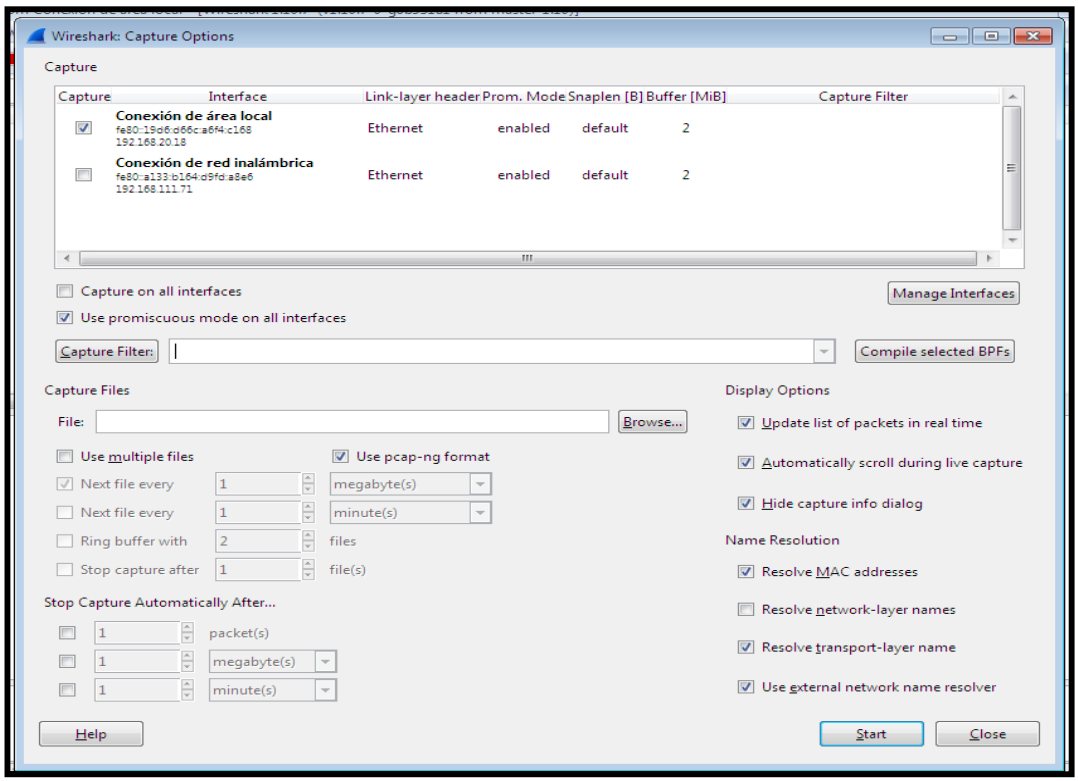



Figura 4.19 Pantalla de opción de Captura Wireshark

Para iniciar la captura de las tramas debemos escoger en Capture options la interface donde será capturado nuestro tráfico, la tarjeta de red deberá ser configurada en modo promiscuo, esto es con el objeto de poder capturar todo el tráfico que se transmita por dicha interface.

Los protocolos que serán objeto de análisis serán el protocolo IPv6, SNMPv1, SNMPv2c y SNMPV3.

### 4.4.1 Análisis del datagrama IPv6

El uso del analizador de protocolo Wirehask en su versión 1.10.7, ya posee soporte para el análisis de la versión del protocolo de internet IPv6 además permite discriminar los protocolos según mi necesidad de análisis.

Entre los protocolos que debemos detectar está el IPv6, para lo cual debemos iniciar la captura de las tramas ejecutando un filtro que muestre este protocolo. En la figura 4.20 muestra el esquema de nuestra red WAN implementada en el simulador GNS3.

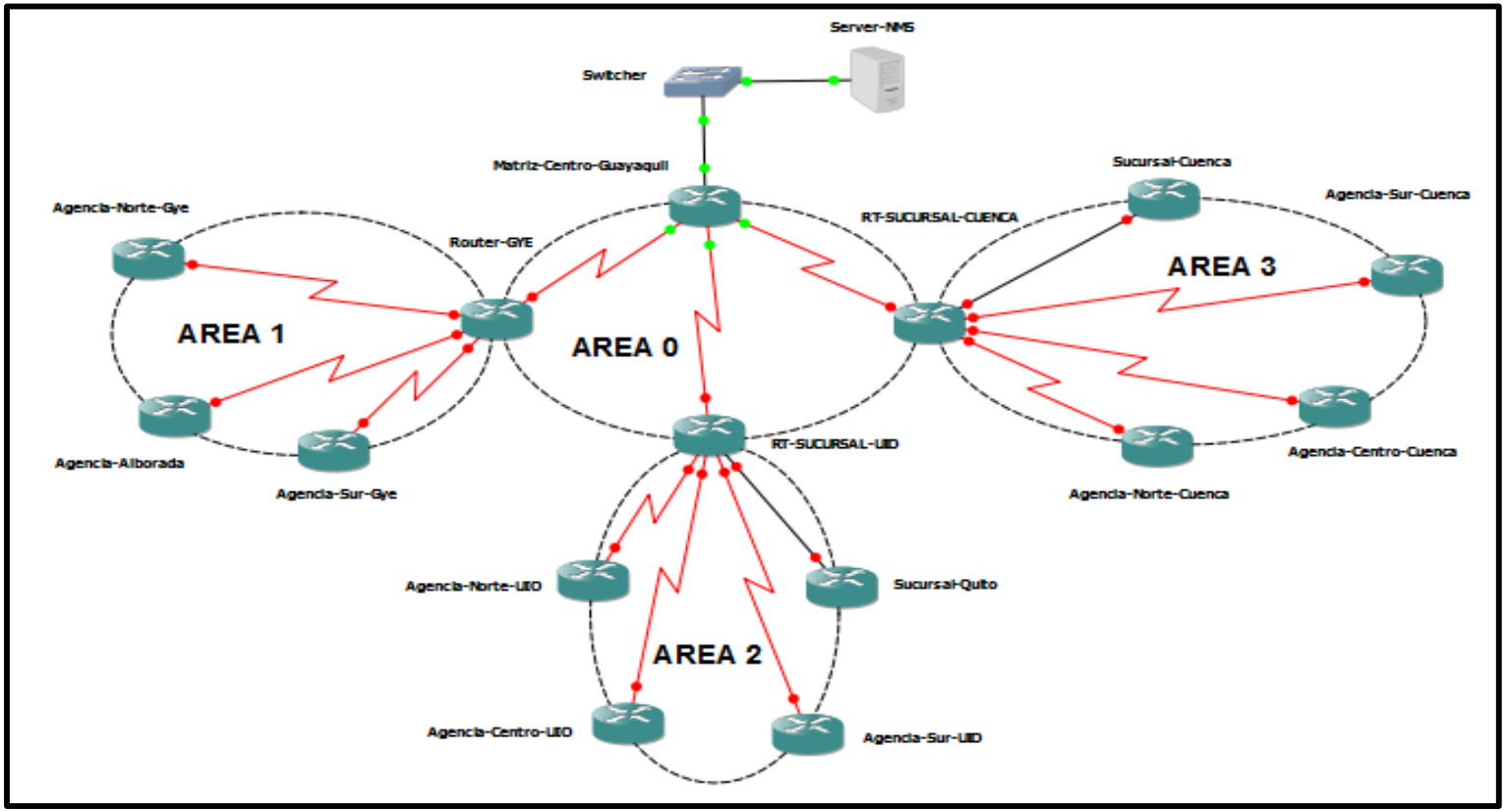



Figura 4.20 Red WAN implementada en GNS3

Podemos observar las direcciones Link-local fe80::786e:11a7:15ba:fa9d, Unique local address fd3a:9a29:9c85:12::1 de nuestro enrutador principal que permite la conexión hacia nuestro servidor NMS fd3a:9a29:9c85:12::2. El análisis con Wireshak como se observa en la Figura 4.21 muestra los protocolos que son transmitido a través de los enlaces hacia las distintas agencias que conforman nuestra red WAN. Y que permite observar el protocolo IPv6 nativo implementado en nuestra red.

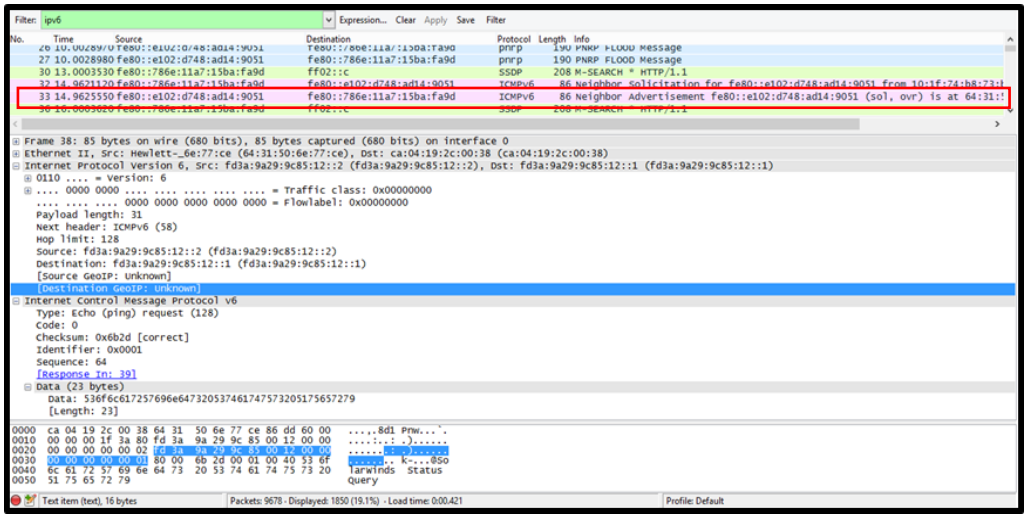



Figura 4.21 Captura del Protocolo de Internet IPv6

Los paquetes que viajan entre nuestros enrutadores como se observa en la Figura 4.22, son ESP (Encapsulating Security Payload) que están encriptados, como se esperaba la transmisión de información a través de nuestra red WAN debe ser cifrada.

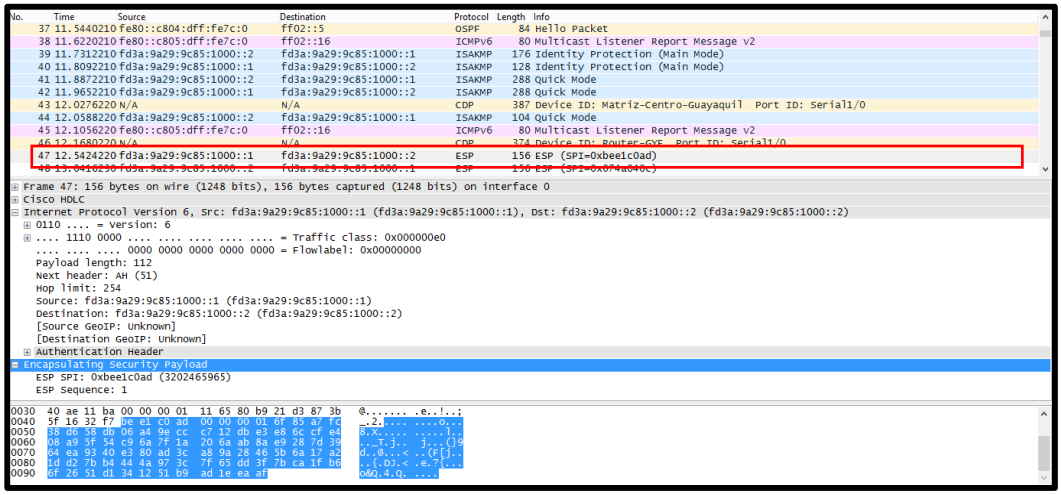



Figura 4.22 Los paquetes entre enrutadores son ESP encriptados.

Una vez que se establecen los túneles entre los enrutadores, podemos observar en la figura 4.23 como funciona el protocolo ISAKMP (Internet Security Association and Key Managment Protocol) con soporte IKE (Internet Key Exchange) utilizado para autenticación e intercambio de claves cuando se establece y se mantiene una conexión IPsec.

Luego de la autenticación se establecen los SA (Security Association) entre los enrutadores. Cada SA define el protocolo IPSec que se utilizara, los algoritmos y claves de encriptación y también su tiempo de vida.

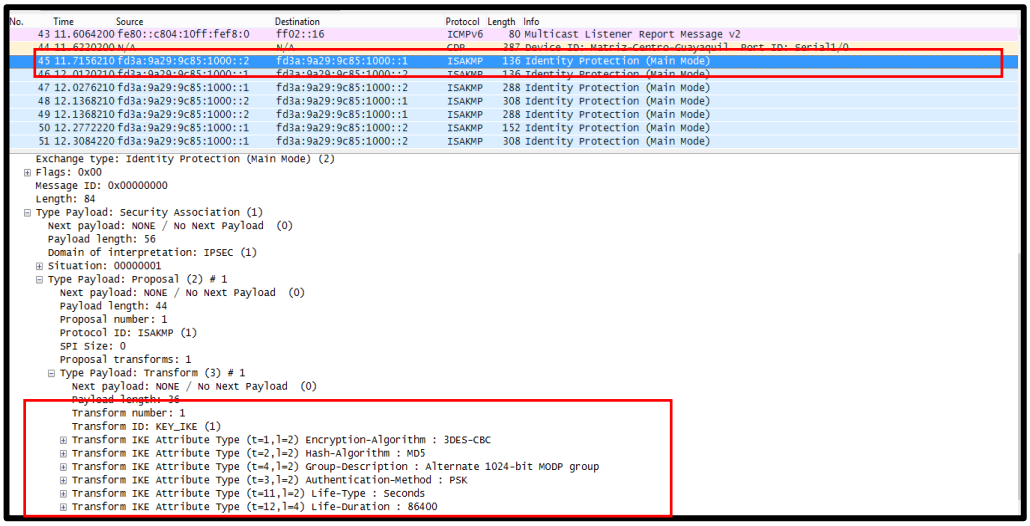



Figura 4.23 Asociación de Seguridad ISAKMP entre enrutadores.

### 4.4.2 Análisis de datagrama SNMPv1.

Una vez configurado los parámetros de SNMPv1 como se indicó en el capítulo 4.3 a cada uno de los enrutadores. Iniciamos nuestro Servidor NMS el cual me permite detectar los enrutadores que forman nuestra red WAN, al iniciar la exploración debemos configurar la versión de SNMP que vamos a utilizar, el software SolarWinds no distingue entre la versión SNMPv1 o SNMPv2c tal como se observa en la figura 4.24, para lograr monitorear la versión SNMPv1 en nuestro enrutador principal solo configuramos esta versión en cada uno de nuestros enrutadores. El resultado de las tramas debemos analizarla en el Wireshak.

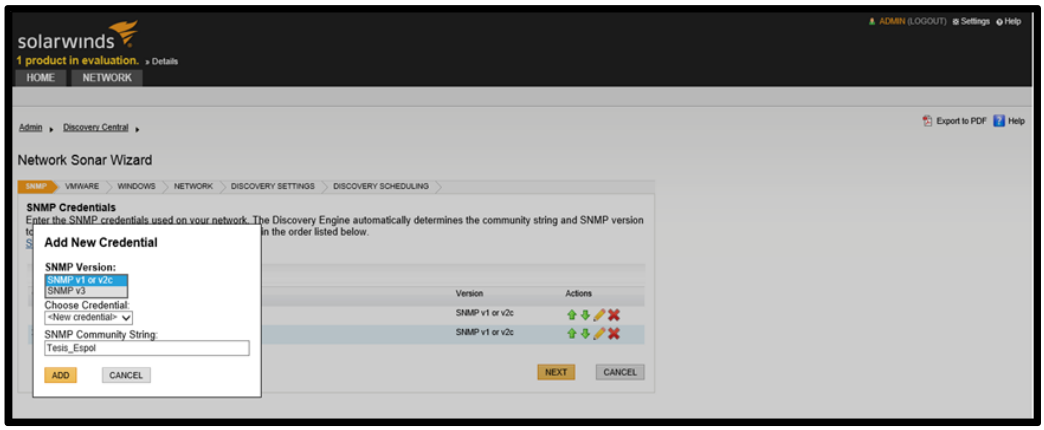



Figura 4.24 Pantalla de selección de Credenciales en SolarWinds.

La exploración de nuestra red WAN la podemos observar en la figura 4.25.

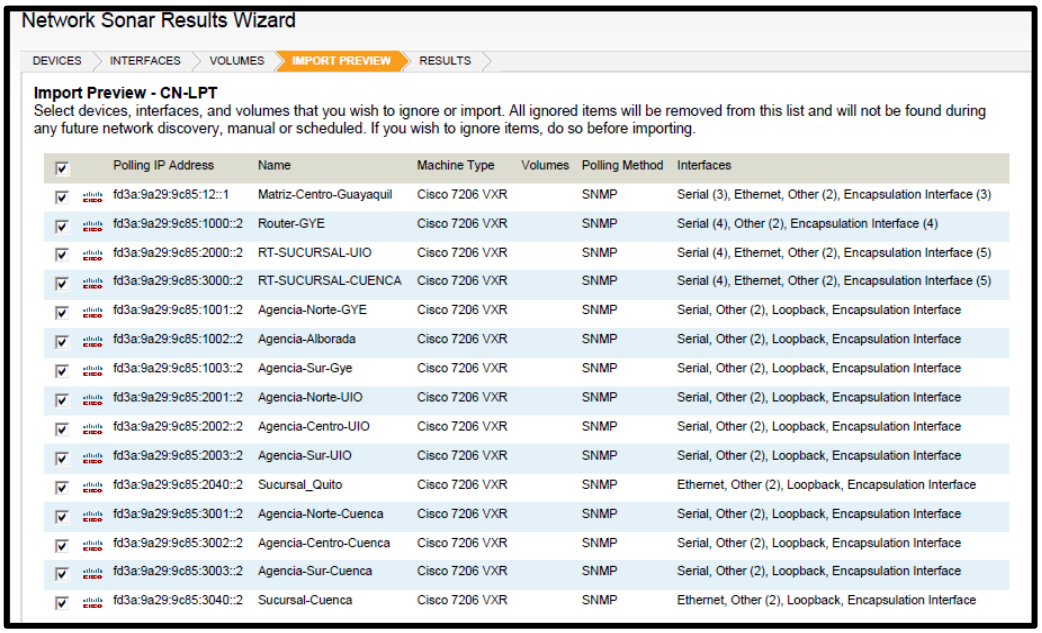



Figura 4.25 Resultado de exploración con Servidor NMS

El análisis con Wireshak se observa un “GetRequest” y “Get-next-request” por parte de nuestro Servidor NMS, obsérvese figura 4.26 y 4.27 respectivamente y un “GetResponse” que es enviado por nuestro enrutador, como se observa en la figura 4.28. Además el enrutador envía un traps hacia nuestro servidor NMS, tal como se observa en la figura 4.29.

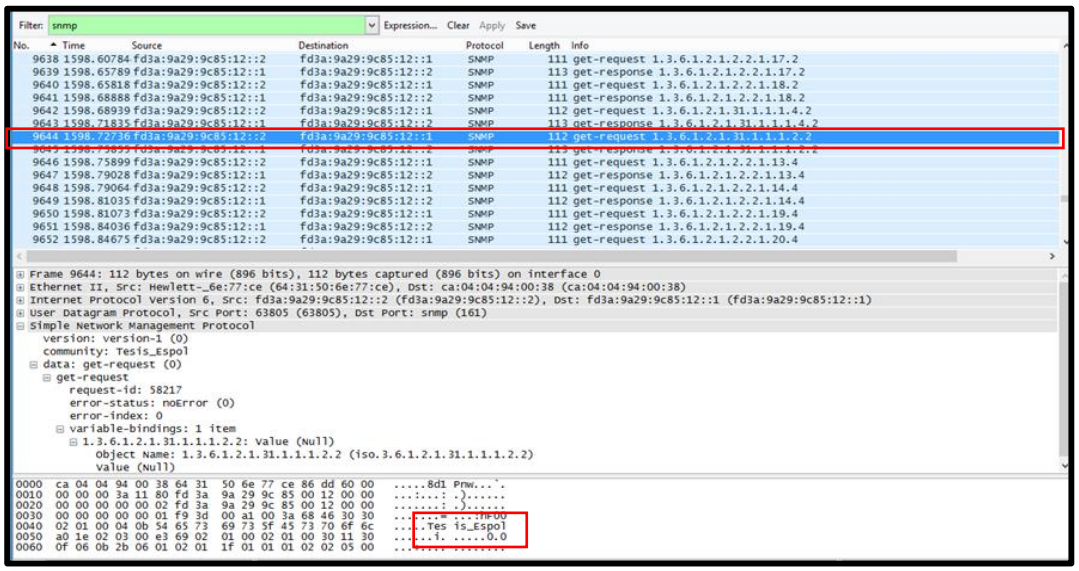



Figura 4.26 Get-request desde el Servidor NMS

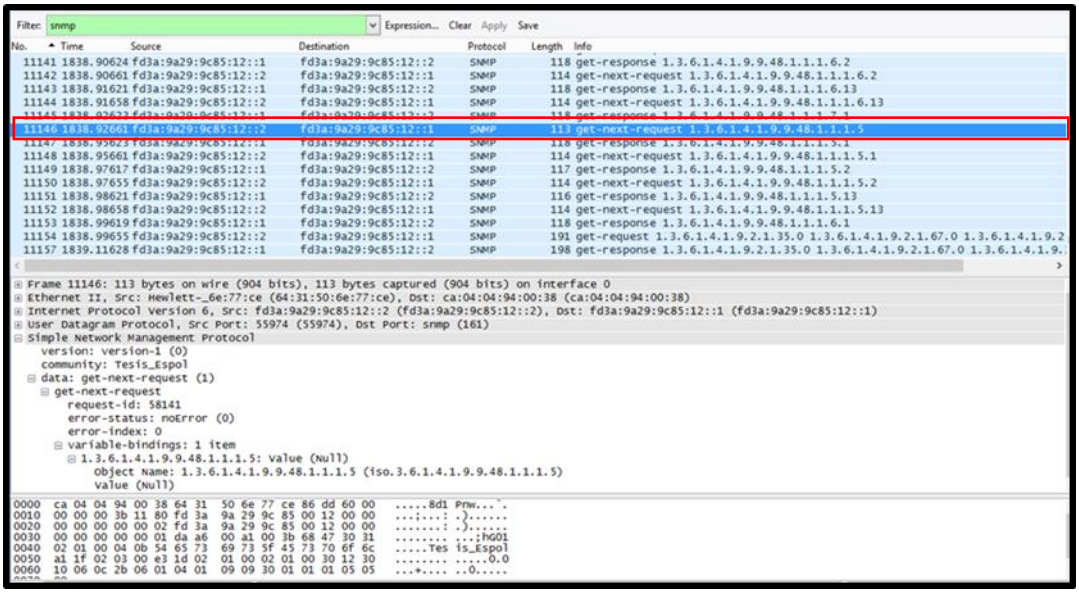



Figura 4.27 get-next-request desde el servidor NMS

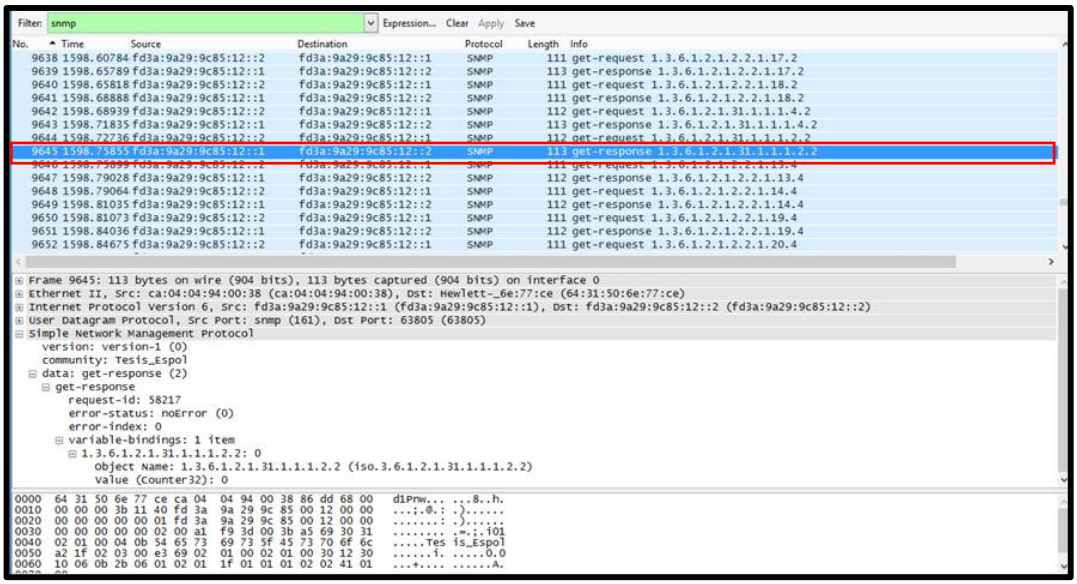



Figura 4.28 Get-response del enrutador Principal

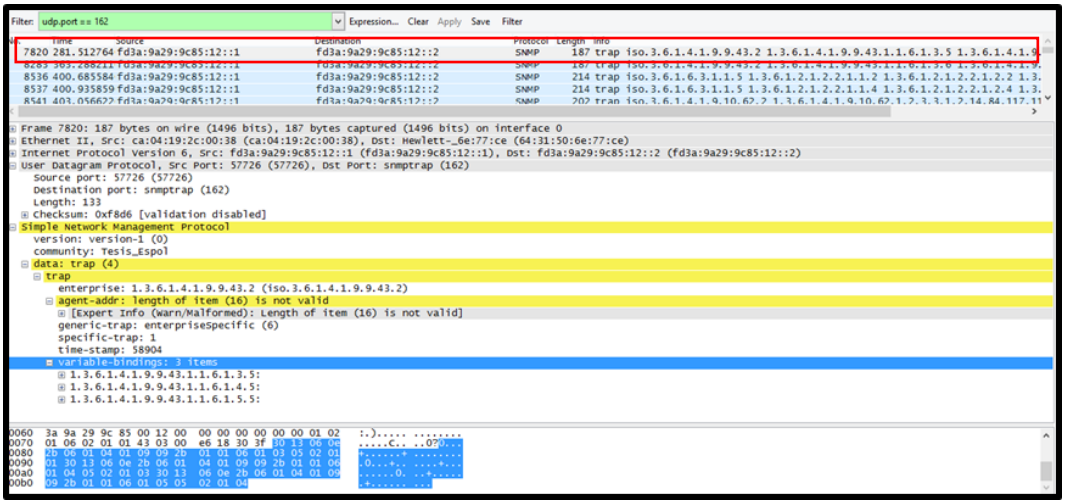



Figura 4.29 Envío de Trap hacia Servidor NMS

### 4.4.3 Análisis de datagrama SNMPv2

El análisis que se realizó a continuación es igual que el anterior; en nuestro servidor NMS se configuró los parámetros de análisis, se ingresó la versión de SNMPV2 y la comunidad. La misma que es Tesis_Espol para todos y cada uno de los enrutadores. Como se puede observar en la figura 4.30. La captura de las tramas con ayuda de Wireshak me permitirá el análisis de los paquetes.

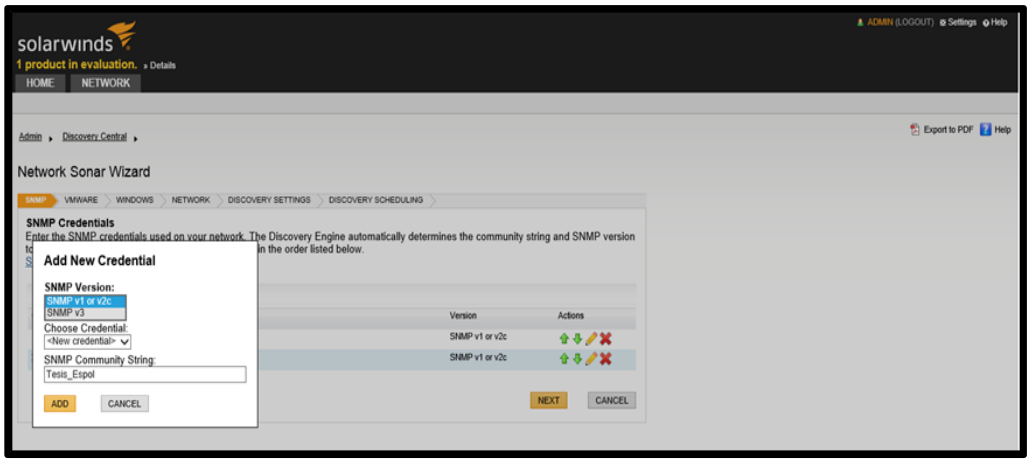



Figura 4.30 Pantalla de selección de Credenciales en SolarWinds

La captura con Wireshak me muestra un GetRequest y un GetNextRequest por parte de nuestro servidor NMS. Véase Figura 4.31, y un GetReponse, como se observa en la Figura 4.32 que es enviado por el enrutador principal.

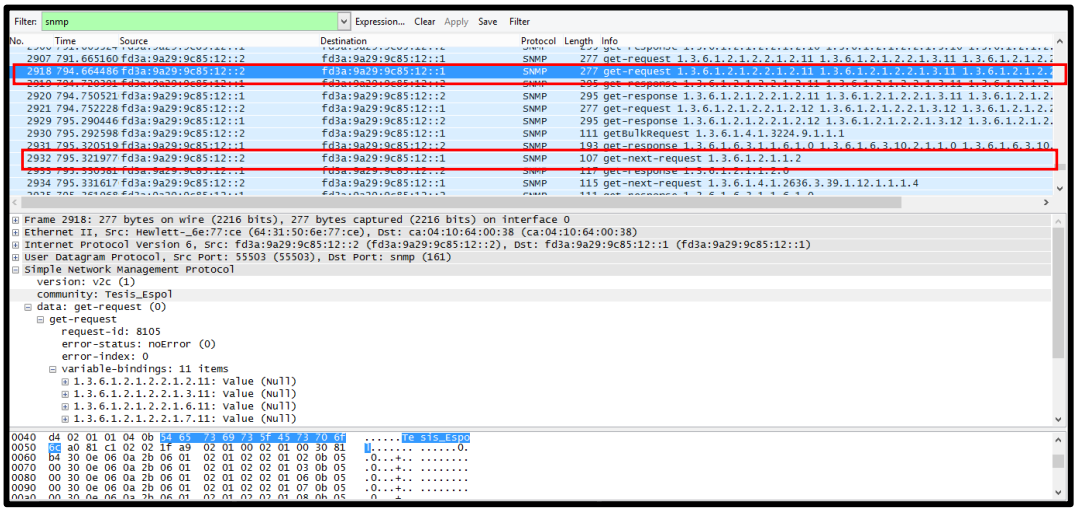



Figura 4.31 Get-request y Get-next-request SNMPv2

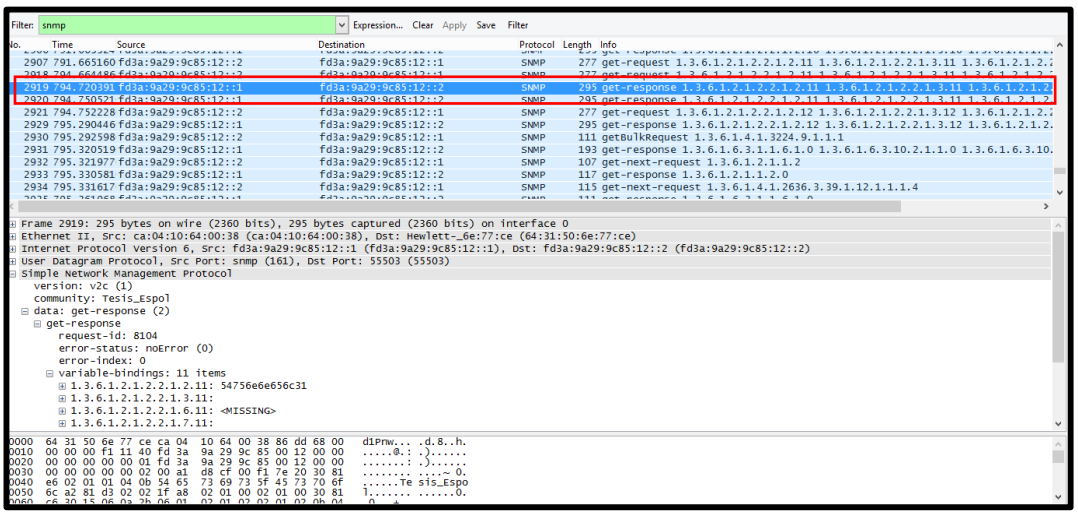



Figura 4.32 Get-response SNMPv2 del enrutador.

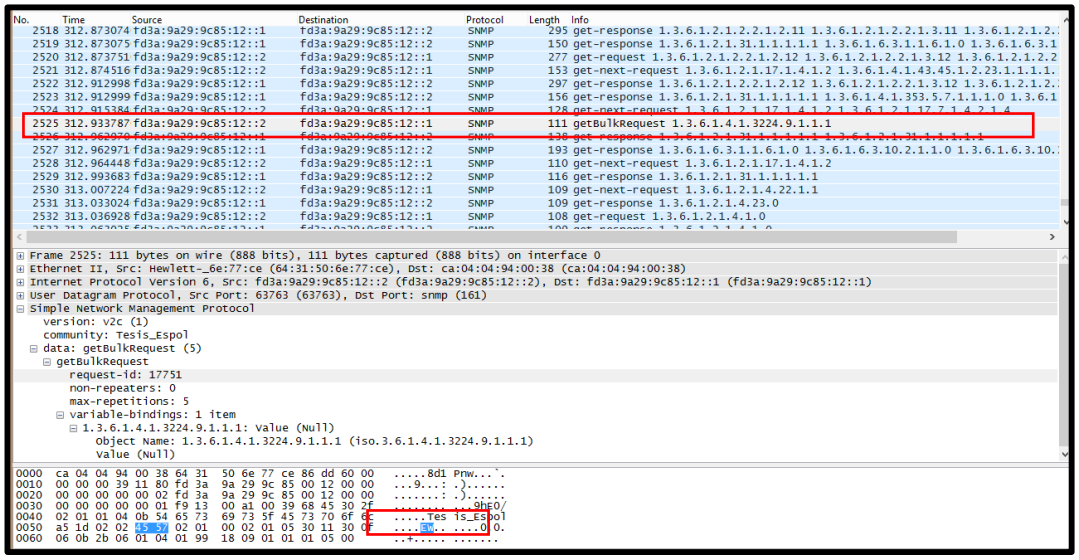


Figura 4.33 GetBulkRequest SNMPv2

En la Figura 4.33 observamos el mensaje getBulkRequest aparece en la versión 2 o 3 cuando se envió una larga transmisión de datos.

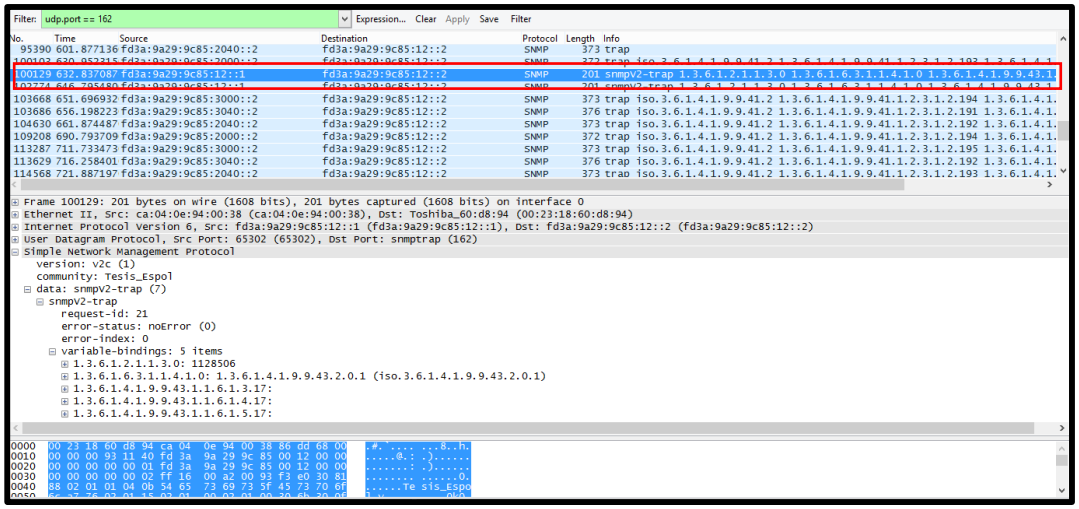


Figura 4.34 Trap SNMPv2 hacia Servidor NMS

### 4.4.4 Análisis del Datagrama SNMPv3

La versión 3 del protocolo SNMP permite ser implementada con tres niveles de seguridad.

- noAuthNoPriv: Comunicación sin autenticación y sin privacidad.
- authNoPriv: Comunicación con autenticación y sin Privacidad.
- authPriv: Comunicación con autenticación y privacidad.

En nuestra red WAN los enrutadores fueron configurados con authPriv es decir, con autenticación para el cual usamos el protocolo MD5 Message-Digest Algorithm 5 y con privacidad que fue implementado con DES (Data Encrytion Standard).

En nuestro Servidor NMS ingresamos las credenciales necesarias para la gestión en el protocolo SNMPv3, el usuario definido en todos los enrutadores Cisco es UserEspol y los protocolos criptográficos son MD5 y DES56. La Figura 4.35 detalla la pantalla de selección de credenciales SNMPv3.

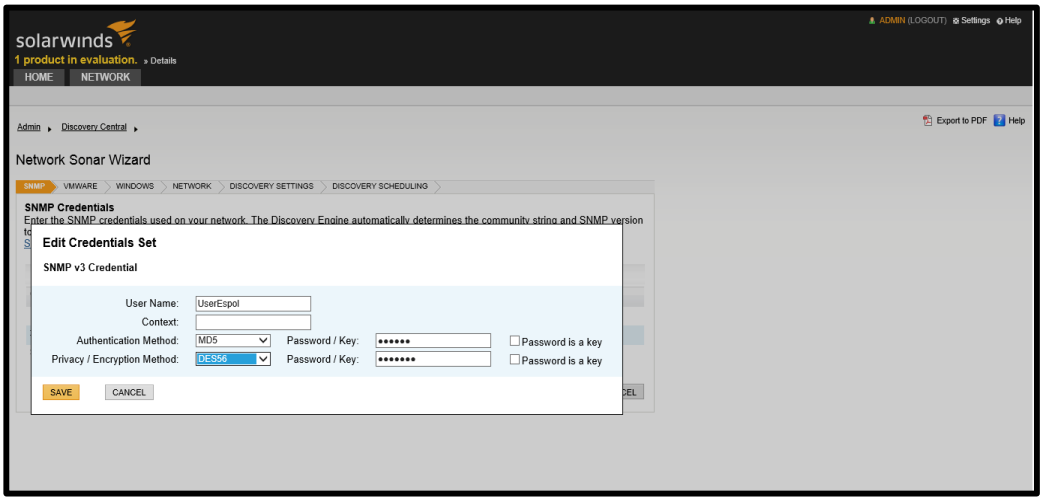



Figura 4.35 Pantalla de selección de Credenciales SNMPv3

Al hacer el análisis de las tramas entre el servidor NMS y enrutador principal, observo en la figura 4.36 el get-request por parte de mi servidor NMS hacia el enrutador principal y a su vez en la figura 4.37 el report que es el mensaje que le devuelve mi enrutador principal.

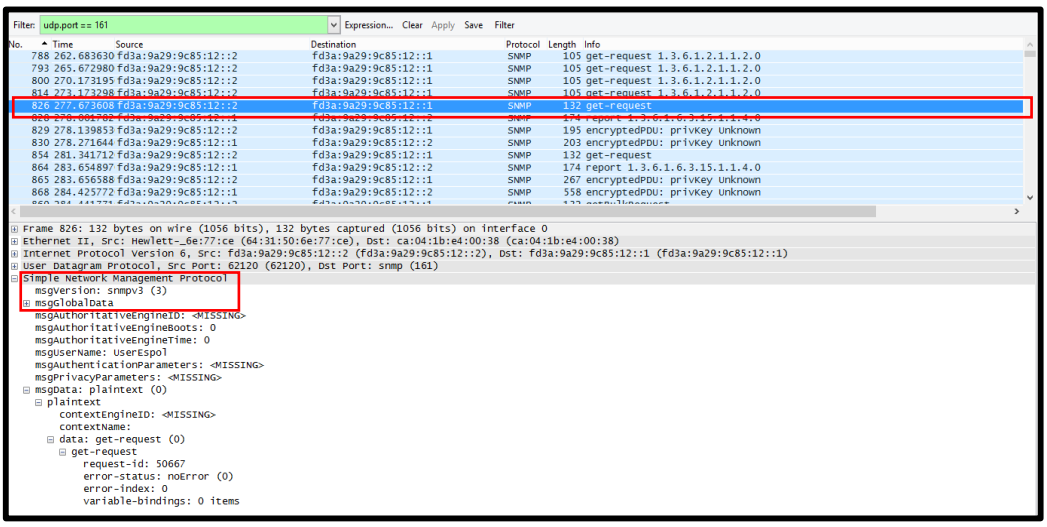



Figura 4.36 Get-request desde Servidor NMS

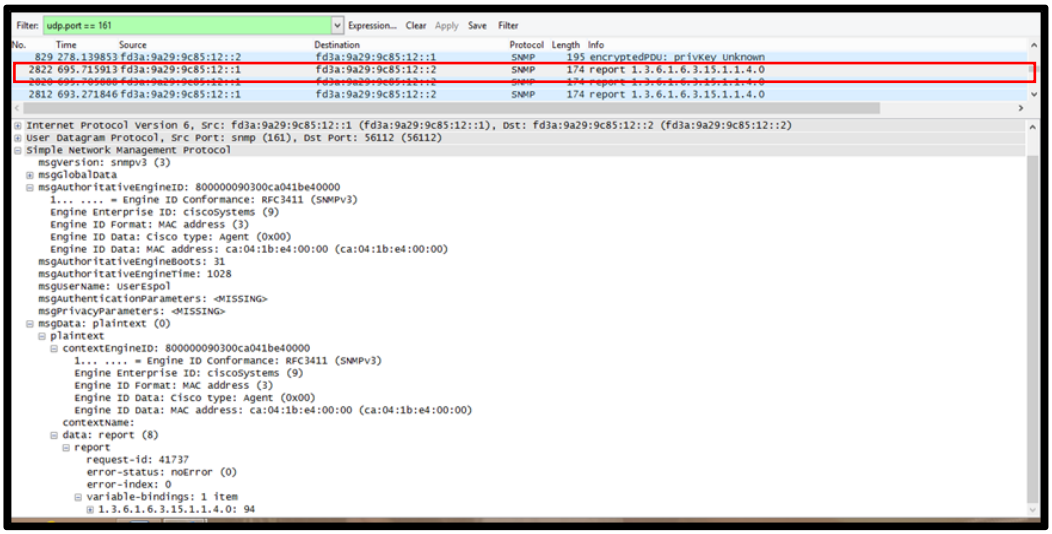



Figura 4.37 Report generado por el enrutador Principal

Las figuras 4.38 y 4.39 muestra él envío de mensajes encriptados entre el servidor NMS y el enrutador principal, se observa los parámetros de encriptación y autenticación.

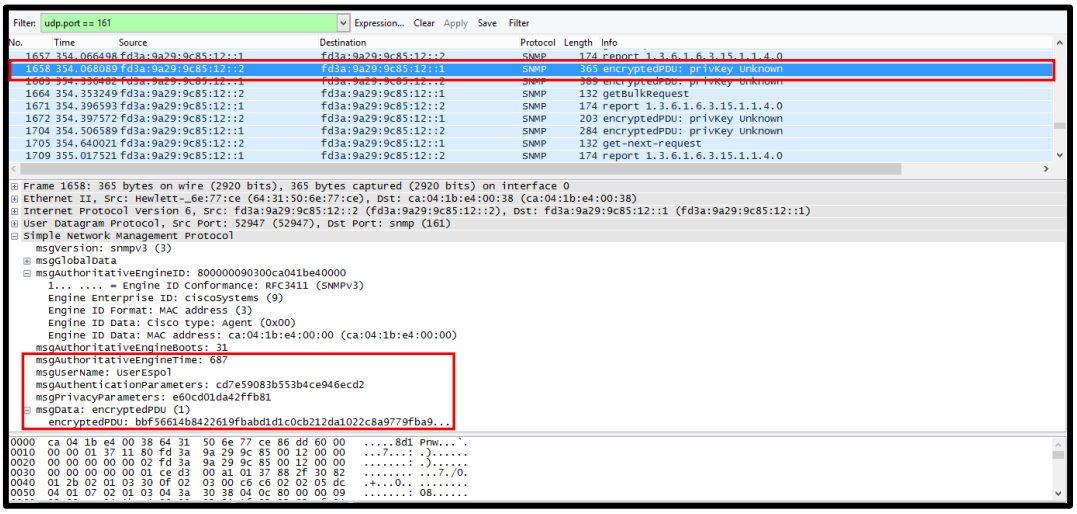



Figura 4.38 PDU Encriptada desde Servidor NMS

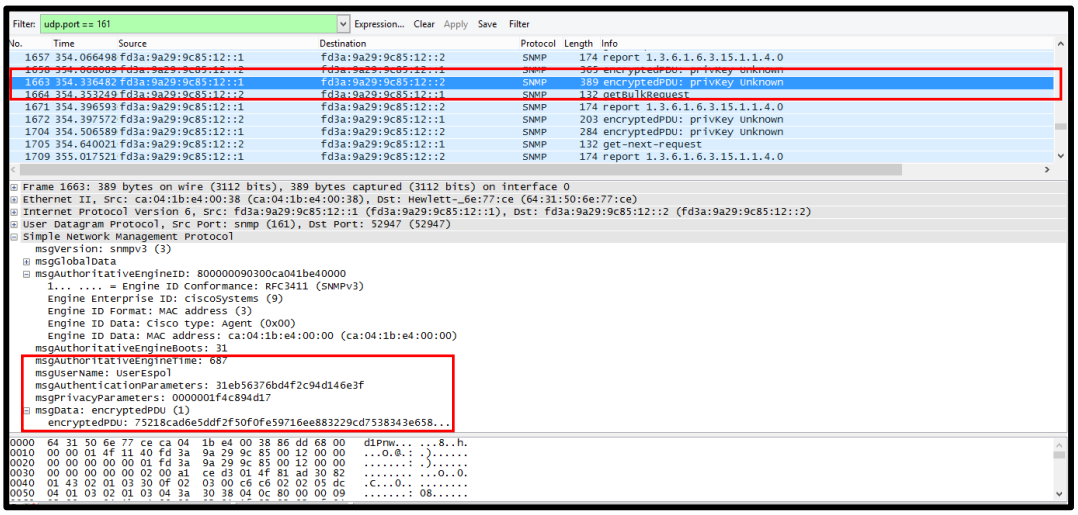



Figura 4.39 PDU Encriptada desde Enrutador Principal

La figura 4.40 muestra el envío de mensaje trap desde el enrutador hacia el servidor NMS. Se observan los parámetros de autenticación y encriptación debidamente cifrados.

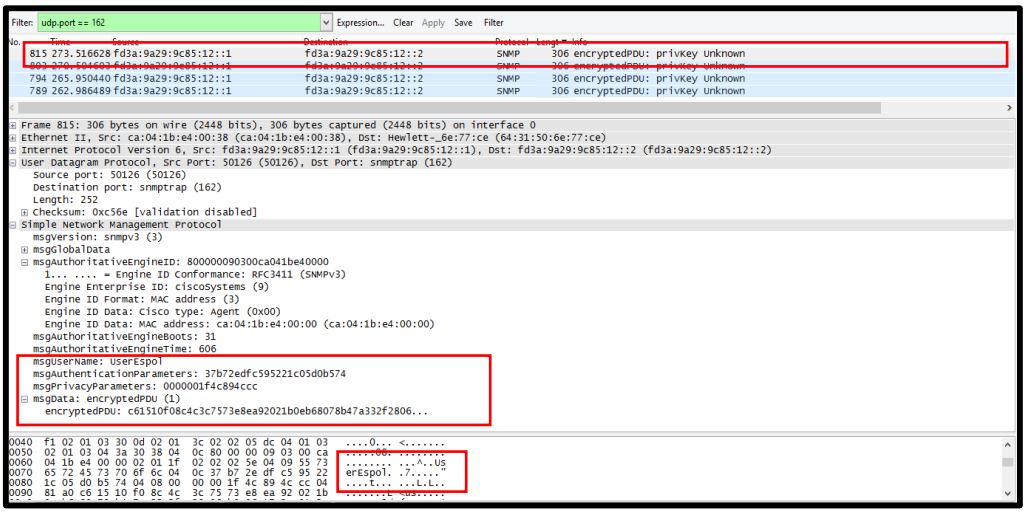



Figura 4.40 Trap Encriptado hacia Servidor NMS

# CAPÍTULO 5

## 5 COSTOS DE IMPLEMENTACION DEL PROYECTO

### 5.1 Costos de hardware (equipos)

En este capítulo analizaremos los costos de los equipos que conforman la red WAN IPV6 del Banco.

La red WAN está conformada jerárquicamente por un enrutador (Router) 3850 que es el principal, 3 Routers 3850 para las ciudades de Guayaquil, Quito y Cuenca ubicados en las sucursales. Y tres router 1950 para las agencias finales.

Cada sucursal y agencia tendrá un Conmutador (Switch) Cisco 2960 de 24 Ptos para crecimiento de la red y segmentación.

Se toma en cuenta además de un equipo Firewall Checkpoint 1100 para cada sucursal y agencia. Y un Checkpoint Firewall IP 690 para la Matriz. Además el costo del Equipo para instalación del NMS, en este caso el NPM de SolarWinds. La Tabla 5.1 muestra el Costo del Hardware.

Tabla 5.1 Costos de Hardware

| | Princ. GYE | GYE Prov. | UIO Prov. | CUE Prov. | Ag. AlboradaGYE | Ag. NorteGYE | Ag. SurGYE | Suc UIO | UIO. Ag. Norte | UIO. Ag. Centro | UIO. Ag. Sur | Suc. CUE | Ag. NorteCUE | Ag. CentroCUE | Ag SurCUE | Cantidad | Costo Unitario | Costo Total |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Router Cisco 3945 | 1 | 1 | 1 | 1 | | | | | | | | | | | | 4 | $ 4.435 | $ 17.740 |
| Router Cisco 1941 | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 11 | $ 1.179 | $ 12.969 |
| Switch Cisco 2960X | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 11 | $ 943 | $ 10.373 |
| Firewall Checkpoint 4400 | 1 | | | | | | | | | | | | | | | 1 | $ 9.789,85 | $ 9.789,85 |
| Firewall Checkpoint 2200 | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 11 | $ 534 | $ 5.874 |
| NMS Server (HP Proliant DL-380 Gen 6) | 1 | | | | | | | | | | | | | | | 1 | $ 4.050 | $ 4.050 |
| | | | | | | | | | | | | | | | | | Subtotal | $ 60.795,85 |
| | | | | | | | | | | | | | | | | | IVA 12% | $ 7.295,5 |
| | | | | | | | | | | | | | | | | | Total | $ 68.091,35 |

## 5.2 Costos de software

El software que usaremos aquí es con licencia del fabricante por un año, para la implementación se usó un equipo HP-Proliant DL-380 Generación 6, Se usó para el mismo una licencia de Windows Server Estándar 2003 y la licencia del Orion NPM de Solarwinds hasta 100 nodos mantenimiento actualizaciones y soporte. En la tabla 5.2 se detalla el Costo del Software.

Tabla 5.2 Costo de Software

| Software | Cantidad | Costo Único | Costo Total |
|---|---|---|---|
| **Windows Server 2003 Estándar** | 1 | $ 604 | $ 604 |
| **Orion NPM hasta 100 nodos** | 1 | $ 2.675 | $ 2.675 |
| | | Subtotal | $ 3.279 |
| | | IVA 12% | $ 393,48 |
| | | Total | $ 3.672,48 |

En total se gasta $ 3.672,48 Dólares para obtener el licenciamiento del servidor con Windows y el Orion NPM.

## 5.3 Costos de implementación.

Para determinar los costos de implementación, se toma en cuenta los costos de instalación e implementación de los Routers (Enrutadores) y de los Firewalls (Muros de Fuego) así como también la instalación e implementación del Sistema Operativo más el NMS - NPM (Orion Network Performance Monitor).

En la implementación se toma en cuenta lo que se denomina una “bodega de horas” en total 25 horas destinadas para la instalación e implementación del proyecto de los Routers, otra bodega de 25 horas para la instalación e implementación del proyecto de los Firewalls y adicional una bodega de 25 horas para la implementación y entrega de monitoreo del Orion NPM. Los costos de Implementación son descritos en la Tabla 5.3

Tabla 5.3 Costos de Implementación

| Software | Costo Único | Costo Total |
|---|---|---|
| **Proyecto Implementación Router´s** | $ 1.500 | $ 1.500 |
| **Proyecto Implementación Firewall´s** | $ 1.500 | $ 1.500 |
| **Proyecto Implementación NMS (Orion NPM)** | $ 1.500 | $ 1.500 |
| | Subtotal | $ 4.500 |
| | IVA 12% | $ 540 |
| | Total | $ 5.040 |

## 5.4 Costos de alquiler de enlaces de última milla con proveedores.

Para alquilar los enlaces debemos de tomar en cuenta lo que es el costo de instalación no recurrente (NRC Non recurring charge) y el costo mensual recurrente (MRC Monthly recurring Charge), los cuales se realizan una sola vez el primero y cada mes el segundo. Se estima los valores para el ejercicio anual. El costo de NRC por instalación de cada uno de los enlaces es de $ 300 dólares. En estos costos ya está incluido el Impuesto al valor Agregado (IVA 12%).

Es de recordar que existen 3 enlaces Sucursales y 9 enlaces a Agencias, los enlaces entre las sucursales y la Matriz son de 8 Mbps, y los enlaces entre las sucursales y cada una de las agencias son de 1 Mbps.

Se tomara en cuenta el costo del alquiler de los enlaces de Las sucursales con la Matriz: Las tablas 5.4 y 5.5 muestran el costo de enlace hacia cada sucursal o Agencias.

Tabla 5.4 Costo Anual Sucursales

| MRC Sucursales | Costo Mensual por Mega | Costo Mensual por 8 Mb Cada Sucursal | Costo Mensual Total Sucursales (3) | Costo Anual Total Sucursales (3) |
|---|---|---|---|---|
| **Proveedor 1 (Costo por Mb)** | . $ 145 | $ 1.160 | $ 3.480 | $ 41.760 |
| **Proveedor 2 (Costo por Mb)** | $ 180 | $ 1.440 | $ 4.320 | $ 51.840 |
| **Proveedor 3 (Costo por Mb)** | $ 900 | $ 7.200 | $ 21.600 | $ 259.200 |

También el costo de alquiler de los enlaces de las agencias hacia las sucursales:

Tabla 5.5 Costo Anual Agencias

| MRC Agencias | Costo Mensual por Mega | Costo Mensual Total Agencias (9) | Costo Anual Total Agencias (9) |
|---|---|---|---|
| **Proveedor 1 (Costo por Mb)** | $ 145 | $ 1.305 | $ 15.660 |
| **Proveedor 2 (Costo por Mb)** | $ 180 | $ 1.620 | $ 19.440 |
| **Proveedor 3 (Costo por Mb)** | $ 900 | $ 9.900 | $ 118.800 |

La suma del costo de las Sucursales y de las agencias da los costos Mensuales Recurrentes Totales (MRC).

## 5.5 Comparación de costos de enlaces.

La suma del costo de las Sucursales y de las agencias da los costos Mensuales Recurrentes Totales (MRC).

Costos Totales (MRC) = Costos Anuales Sucursales + Costos anuales agencias.

Costos Totales (NRC) = Costos por instalación de cada enlace x número de enlaces (Agencias más Sucursales), en este caso cuesta $300 dólares cada enlace instalado por el proveedor. La tabla 5.6 muestra una comparación de costos entre diversos proveedores.

Tabla 5.6 Comparación de Costos Proveedores

| **Costo Proveedores** | **Proveedor N1** | **Proveedor N2** | **Proveedor N3** |
|---|---|---|---|
| NRC (Dolares) | $ 3.600 | $ 3.600 | $ 3.600 |
| MRC (Dolares) | $ 57.420 | $ 70.920 | $ 378.000 |
| SLA | 99.85 % | 99.80 % | 99.85 % |
| Packet Loss | 0% | 0% | 0% |
| Delay Circuito Nacional (ms) | 3 ms | 5 ms | 4 ms |
| Costo Total enlaces (NRC+MRC) | $ 61.020 | $ 74.520 | $ 381.600 |

## 5.6 Comparación de costos de software de gestión.

El software de Gestión a Nivel empresarial se lo lleva con costos de Instalación y Mantenimiento con licencia anual como es el caso del Orion Network Performance Monitor (NPM) de SolarWinds. Realizaremos la comparación con el que se considera el más completo de los NMS a nivel empresarial que es el NNMi de HP, también con software de gestión de red OpenSource como son el Nagios, el Cacti y el JFFNMS.

Nuestro proyecto necesita de la revisión de hasta 100 interfaces, dentro de los 15 nodos (Router) que se está monitoreando. La tabla 5.7 muestra un análisis comparativo de costo de diversas soluciones de Software de Gestión.

Tabla 5.7 Valores Software de Gestión

| | HP - NNMi ISPi | Orion NPM | Nagios | Cacti | JFFNMS |
|---|---|---|---|---|---|
| **Licencia 100 Nodos Anual** | $ 10.334 | $ 2.675 | 0 | 0 | 0 |
| **Licencia 250 Nodos Anual** | $ 10.334 | $ 5.475 | 0 | 0 | 0 |
| **Licencia de 500 Nodos Anual** | $ 20.668 | $ 8.475 | 0 | 0 | 0 |

Se demostró en capítulos anteriores que el software open source trabaja muy bien con la versión IPV4 y podría trabajar a nivel empresarial,

pero con IPV6 no está madura, por lo que se decidió utilizar el Orion NPM de Solarwinds que trabaja muy bien con el Stack IPV6 y comparado con el HP NNMi ISPi, que también lo hace, la licencia de los 100 nodos o interfaces, el Orion NPM cuesta solo el 25,88% del valor del HP NNMi (Network Node Manager), fuera de la curva de aprendizaje entre uno y otro y el tiempo de implementación, que son mayores en el HP NNMi ISPi.

Resumen de Costos Totales.

Para realizar este resumen, se escogió la licencia de Orion NPM de SolarWinds de 100 nodos y para el alquiler de los enlaces se tomó en cuenta el de menor retardo y el SLA más alto ofrecido por el proveedor N2. Como se muestra en la tabla 5.8.

Tabla 5.8 Resumen de Costos Totales.

| **Resumen de Costos Totales** | |
|---|---|
| **Costos de Hardware** | $ 68.091,35 |
| **Costos de Software** | $ 3.672,48 |
| **Costos de Implementación del proyecto** | $ 5.040,00 |
| **Costos de Alquiler Anual de Enlaces (Proveedor N2)** | $ 74.520,00 |
| **Total** | $ 151.323,83 |

En total los costos del proyecto son de $ 151.323,83 dólares americanos, para poder levantar la infraestructura WAN de la Institución Bancaría Piloto.

# CONCLUSIONES

1. Al usar ULA (Unical local address) nos aseguramos que las direcciones IPv6 asignadas en cada uno de los enrutadores, no serán publicadas en Internet.

2. Se validó que las tramas entre los enrutadores que usan IPsec con IPv6 viajan encriptadas, con lo cual se asegura la confidencialidad de la información.

3. El tráfico SNMP v1 y v2c funcionan correctamente con la pila IPV6 y viajan en formato de texto plano, es decir sin encriptación.

4. El tráfico SNMPV3 funciona correctamente con la Pila IPV6 y que hay una mejora respecto a las versiones anteriores, porque se autentica por usuario, y se puede enviar encriptado o sin encriptar, por ser un ambiente Bancario y para asegurar la data se lo envía encriptado.

5. El software de Gestión de Red (NMS), que se implemento es el Orion Network Performance Monitor (NPM) ya que las soluciones “Open source” no están maduras respecto a IPV6 y no levantan estadísticas de tráfico.

6. El Orión NPM es un software de Gestión Maduro y de fácil despliegue en un entorno empresarial y tiene soporte nativo de IPV6, por lo cual no hay inconvenientes para colectar la data y graficarla.

7. El Orion NPM en comparación con el HP NNMi es más barato respecto al licenciamiento, como se ve en las estadísticas o costos de hasta 100 nodos.

8. Se considera 75 horas de proyecto entre la instalación de los enrutadores, la instalación e implementación de los firewalls y el despliegue del Servidor y software de gestión de Red.

# RECOMENDACIONES

1. Se recomienda trabajar con software Orion NPM (propietario) para trabajar con IPV6, pues las soluciones Open Source no son tan amigables y no usan la pila IPV6 por lo tanto no realizan gráficos.

2. Las configuraciones de todos los equipos que forman parte de la WAN Corporativa Bancaria, deben de realizarse con encriptación entre los nodos.

3. Para la simulación de la red Bancaria a través del GNS3 se recomienda un equipo con características de empresa, pues los consumos en procesador y memoria son altos.

4. Se recomienda usar el SNMP V3 por asuntos de seguridad y evitar el uso de la SNMP V1 y SNMP V2.

# BIBLIOGRAFÍA

[1] Ortega, L. (2011). Caracteriticas IPv6. Obtenido de http://ipv6-equipo5.blogspot.com/p/caracteristicas.html

[2] Deering, S., & Hinden, R. (1998). Request for Comments, 2460. Protocolo IPv6. Obtenido de http://tools.ietf.org/html/rfc2460#section-1

[3] Postel, J. (Septiembre de 1981). Protocolo de Internet IPv4. Obtenido de http://www.ietf.org/rfc/rfc791.txt

[4] Palet Martinez , J. (2010). Tutorial IPv6. Obtenido de http://www.consulintel.es/Html/ForoIPv6/Documentos/Tutorial%20de%20IPv6.pdf Pag. 1-5

[5] Hinden, R; Deering, S;. (Febrero de 2006). Request for Comments, 4291.IPv6 Arquitectura de Direccionamiento. Obtenido de http://www.cu.ipv6tf.org/rfcs/rfc4291.txt

[6] Portal IPv6 Cuba. (2013). Obtenido de http://www.6ip.cu/direccionamientoipv6.htm

[7] Huitema, C; Carpenter, B. (Septiembre de 2004). Request for Comments: 3879, Deprecating Site Local Addresses. Obtenido de http://tools.ietf.org/html/rfc3879

[8] Hinden, R; Haberman, B;. (Octubre de 2005). Request for Comments: 4193, Unique Local IPv6 Unicast Addresses. Obtenido de http://tools.ietf.org/html/rfc4193

[9] Jara Saba, F. E. (Abril de 2009). Estudio e Implementación de una Red IPv6 en la UTFSM. Obtenido de http://www.share-pdf.com/e7fea698e87e43dbbcb6c98d132037b5/ImplementacionIpv6_UTFSM_proyecto.pdf

[10] Kashimura, Yasuo;. (2010). *IPv6 Multicast Tutorial.* Obtenido de http://meetings.apnic.net/__data/assets/pdf_file/0009/18855/IPv6-Multicast-for-CarrierISP-Tutorial_Yasuo-Kashimura.pdf

[11] Hinden, R; Deering, S; Nordmark, E;. (Agosto de 2003). *Request for Comments: 3587, Direcciones Unicast Globales.* Obtenido de http://www.6ip.cu/rfcs/rfc3587.txt

[12] Cisco Systems, Inc.;. (2005). IPv6 Routing. Obtenido de http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd80260051.pdf

[13] Conta, A., & Deering, S. (Marzo de 2006). *request for Comments: 4443, Protocolo de Mensajes de Control de Internet v6.* Obtenido de http://tools.ietf.org/html/rfc4443

[14] Narten, T; Nordmark, E; Simpson, W; Soliman, H. (Septiembre de 2007). *Request for Comments: 4861, Protocolo de descubrimiento de Vecinos.* Obtenido de http://tools.ietf.org/html/rfc4861

[15] Palet Martinez, J., & Cabellos-Aparicio, A. (Enero de 2004). El Protocolo IPv6. Obtenido de http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf Pag. 13-16

[16] Kent, S; Atkinson, R;. (Agosto de 2005). *Request for Comments: 2401,* Arquitectura de Seguridad para el Protocolo Internet. Obtenido de http://www.rfc-es.org/rfc/rfc2401-es.txt

[17] Vasquez Clavijo, J. E. (Abril de 2011). *Analisis de las funcionalidades de los Protocolos de Seguridad IPsec.* Obtenido de http://dspace.ups.edu.ec/bitstream/123456789/1683/8/UPS-ST000292.pdf Pag 79, 80.

[18] Alcocer Garcia, C. (2000). Seguridad en Redes de Computadoras. Obtenido de http://biblioteca.pucp.edu.pe/docs/elibros_pucp/alcocer_carlos/24_Alcocer_2000_Redes_Cap_24.pdf Pag 352-358

[19] Perez Iglesias, S. (Noviembre de 2001). *Analisis del Protocolo IPSec: El estandar de la seguridad en IP.* Obtenido de http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/IPSec/ipsec.pdf Pag. 52-57

[20] Alvarado Ortiz, A. E., Gonzalez Requena, S. E., & Taracena Pinzon, J. A. (Marzo de 2004). Analisis del Protocolo IPsec, Seguridad Basada en Criptografia. Obtenido de http://www.tesis.ufm.edu.gt/pdf/3930.pdf

[21] Barba Marti, Antoni;. (1999). *Gestion de Red.* Barcelona, España: Edicions de la Universitat Politecnica Catalunya, SL. Pag. 15, 16, 76, 89.

[22] Millan Tejedor, R. J. (1999). *Gestion de Red.* Obtenido de http://www.ramonmillan.com/tutoriales/gestionred.php#Arquitectura

[23] Valle Vidal, P. E. (Agosto de 2007). *Diseño e Implementacion de un Sistema de Monitoreo Basado en SNMP para una red de Telefonia IP Asterisk.* Obtenido de http://profesores.elo.utfsm.cl/~tarredondo/memorias/2007-memoria-pvalle.pdf

[24] Mauro, Douglas R; Schmidt, Kevin J. (July de 2001). *Essential SNMP, First Edition.* Obtenido de http://docstore.mik.ua/orelly/networking_2ndEd/snmp/index.htm

[25] Crespata Almachi, R. A. (Agosto de 2012). *Analisis del Protocolo SNMPv3 para el desarrollo de un prototipo de monitoreo de Red Segura.* Obtenido de http://dspace.espoch.edu.ec/handle/123456789/2037

[26] Velasquez Cruz, A. S. (Febrero de 2009). Diseño e implementacion de un modulo software para la monitorizacion de elementos de una Red informatica utilizando el protocolo SNMP y el lenguaje XML. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/1135/1/CD-1981.pdf

[27] Lorenzo Álvarez, D. (2011). Monitorización de Red con SNMP y MRTG. Obtenido de http://www.slideshare.net/francescperezfdez/monitorizacin-de-red-con-snmp-y-mrtg#

[28] Harrington, D; Presuhn, R; Wijnen, B;. (Diciembre de 2002). Request for Comments: 3411, Arquitectura SNMPv3. Obtenido de http://www.ietf.org/rfc/rfc3411.txt

[29] Blumenthal, U; Wijnen, B;. (Diciembre de 2002). *Request for Comments: 3414, Modelo de Seguridad basado en Usuario. SNMPv3.* Obtenido de http://tools.ietf.org/html/rfc3414

[30] Cisco Systems;. (2012). *IPv6 Configuration Guide, Cisco IOS.* Obtenido de http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6/configuration/15-2mt/ipv6-15-2mt-book.pdf

[31] Solar Winds. (2014). *Solar Winds*. Obtenido de http://www.solarwinds.com/es/#network

[32] Nagios. (2014). *Nagios.org*. Obtenido de http://www.nagios.org/

[33] Just For Fun Network Management System. (2014). *Just For Fun Network Management System*. Obtenido de http://www.jffnms.org/

[34] Hidalgo, Julio Cesar; Jaramillo, Sebastian;. (2010). Seguridad en IPv6. Obtenido de http://www.supertel.gob.ec/pdf/Consideraciones%20de%20Seguridad%20para%20Implementacion%20de%20IPv6%20FA.pdf Pag. 5-8

# ANEXO A

El anexo siguiente nos muestra en detalle los comandos de configuración de lo enrutadores Cisco y los parámetros de configuración establecidos en el enrutador principal.

COMANDOS DE CONFIGURACION BÁSICA

| **CONFIGURACION DE DIRECCIONES IPv6** | |
|---|---|
| Comando o Acción | Propósito |
| **Enable**<br>Ejemplo:<br>Router> enable | Habilita executar en modo privilegiado |
| Comando o Acción | Propósito |
| **Configure terminal**<br>Ejemplo:<br>Router# configure terminal | Ingresa al modo de configuración global |
| Comando o Acción | Propósito |
| **interface** *type number*<br>Ejemplo:<br>Router(config)# interface serial 1/0 | Especifica el tipo de interfaz y el número, y coloca el dispositivo en el modo de configuración de interfaz<br>. |
| Comando o Acción | Propósito |
| **ipv6 address** *ipv6-prefix/prefix-length*<br>Ejemplo:<br>Router(config)# ipv6 address *FD3A:9A29:9C85:12::1*<br>**ipv6 enable** | Especifica una red IPv6 asignada a la interfaz y permite el procesamiento de IPv6 en la interfaz. Configura automáticamente una dirección local de enlace IPv6 en la interfaz y habilita la interfaz para el procesamiento de IPv6 |
| Comando o Acción | Propósito |
| **exit**<br>Ejemplo:<br>Router(config-if)# exit | Sale del modo de configuración de interface y retorna al modo de configuración global. |

COMANDOS DE CONFIGURACION IPSEC

| **CREACION DE UNA POLITICA IKE Y UNA PRESHARED KEY EN IPv6** | |
|---|---|
| Comando o Acción | Propósito |
| **enable**<br>Ejemplo:<br>Router> enable | Habilita executar en modo privilegiado |
| Comando o Acción | Propósito |
| **configure terminal**<br>Ejemplo:<br>Router# configure terminal | Ingresa al modo de configuración global |
| Comando o Acción | Propósito |
| **crypto isakmp policy** *priority*<br>Ejemplo:<br>Router(config)# crypto isakmp policy 4 | Define la política de intercambio de IKE y entra en el modo de configuración ISAKMP.<br>Política número 1 indica una política con alta prioridad. |
| Comando o Acción | Propósito |
| **authentication {rsa-sig \| rsa-encr \| pre-share}**<br>Ejemplo:<br>Router(config-isakmp-policy)# authentication pre-share | Especifica el método de autentificación dentro de una política<br>IKE.<br>***rsa-sig*** y ***rsa-encr*** *no son soportados en IPv6.* |
| Comando o Acción | Propósito |
| **hash { sha \| md5 }**<br>Ejemplo:<br>Router(config-isakmp-policy)# hash md5 | Especifica el algoritmo hash dentro de una política IKE. |
| Comando o Acción | Propósito |
| **group { 1 \| 2 \| 5 }**<br>Ejemplo:<br>Router(config-isakmp-policy)# group 2 | Especifica la identificación del grupo Diffie-Hellman dentro de una política IKE. |

| Comando o Acción | Propósito |
|---|---|
| **encryption { des \| 3des \| aes \| aes 192 \| aes 256 }**<br>Ejemplo:<br>Router(config-isakmp-policy)# encryption 3des | Especifica el algoritmo de encrytacion dentro de una política<br>IKE. |
| Comando o Acción | Propósito |
| **lifetime** *seconds*<br>Ejemplo:<br>Router(config-isakmp-policy)# lifetime 86400 | Especifica el tiempo de vida de una IKE dentro de una asociación de seguridad. |
| Comando o Acción | Propósito |
| **exit**<br>Ejemplo:<br>Router(config-isakmp-policy)# exit | Entre este comando para salir del modo de configuración ISAKMO policy al modo de configuración global. |
| Comando o Acción | Propósito |
| **crypto isakmp keepalive 30 30**<br>Ejemplo:<br>Router(config)# crypto isakmp keepalive 30 30 | |
| Comando o Acción | Propósito |
| **cryto isakmp key enc-type-digist keystring { address peer-address** [mask] \| ipv6 {ipv6-address/ipv6-prefix} \| hostname hostname} [no-xauth]<br>Ejemplo:<br>Router(config)# crypto isakmp key 6 my-preshare-key-0 address ipv6 FD3A:9A29:9C85:1000::2/64 | Configura una clave previa de autenticación. |
| Comando o Acción | Propósito |
| **end**<br>Ejemplo:<br>Router(config-crypto)# exit | Sale del modo de configuración cryto keyring y retorna al modo privilegiado. |

COMANDOS DE CONFIGURACION TRANSFORM SET

| **CONFIGURACION de Ipsec Transform Set and Ipsec Profile** | |
|---|---|
| Comando o Acción | Propósito |
| **enable**<br>Ejemplo:<br>Router> enable | Habilita executar en modo privilegiado |
| Comando o Acción | Propósito |
| **configure terminal**<br>Ejemplo:<br>Router# configure terminal | Ingresa al modo de configuración global |
| Comando o Acción | Propósito |
| **crypto ipsec transform-set** *transform-set-name transform1 [transform2]* [transform3] [transform4]<br>Ejemplo:<br>Router(config)# crypto ipsec transform-set myset0 ah-sha-hmac esp-3des | Define un conjunto de transformación y coloca el router en el modo de configuración de transformación criptográfica. |
| Comando o Acción | Propósito |
| **crypto ipsec profile** *name*<br>Ejemplo:<br>Router(config)# crypto ipsec profile profile0 | Define los parámetros de Ipsec que se van a utilizar para el cifrado Ipsec entre dos routers Ipsec. |
| Comando o Acción | Propósito |
| **set transform-set** *transform-set-name [transform-set-name2.. transform-set-name6]*<br>Ejemplo:<br>Router(config-crypto-transform)# set transform-set myset0 | Específica que conjuntos de transformación con la entrada. |
| Comando o Acción | Propósito |
| **end**<br>Ejemplo:<br>Router(config-crypto-transform)# end | Sale del modo de cifrado de trasformación y vuelve al modo privilegiado. |

COMANDOS DE CONFIGURACION TUNEL IPsec

| **CONFIGURACION TUNNEL IPsec** | |
|---|---|
| Comando o Acción | Propósito |
| **enable**<br>Ejemplo:<br>Router> enable | Habilita executar en modo privilegiado |
| Comando o Acción | Propósito |
| **configure terminal**<br>Ejemplo:<br>Router# configure terminal | Ingresa al modo de configuración global |
| Comando o Acción | Propósito |
| **ipv6 unicast-routing**<br>Ejemplo:<br>Router(config)#ipv6 unicast-routing | Habilita el intercambio de datagramas unicast IPv6. |
| Comando o Acción | Propósito |
| **interface tunnel** *tunnel-number*<br>Ejemplo:<br>Router(config)# interface tunnel 0 | Especifica un número a la interfaz de túnel y entra en el modo de configuración de interfaz. |
| Comando o Acción | Propósito |
| **interface ospf # area #**<br>Ejemplo:<br>Router(config)#interface ospf 1 area 0 | |
| Comando o Acción | Propósito |
| **ipv6 address** *ipv6-address/prefix*<br>Ejemplo:<br>Router(config-if)# ipv6 address FD3A:9A29:9C85:1041::1/64 | Proporciona una dirección IPv6 a la interfaz de túnel, por lo que el trafico IPv6 se puede dirigir a ese túnel. |

| Comando o Acción | Propósito |
|---|---|
| **ipv6 enable**<br>Ejemplo:<br>Router(config-if)# ipv6 enable | Habilita IPv6 en esta interfaz de túnel. |
| Comando o Acción | Propósito |
| **tunnel source** *{ip-address \|ipv6-address \| interface-type interface-number}*<br>Ejemplo:<br>Router( config-if) # tunnel source serial 0/0 | Establece la dirección de origen para una interfaz de túnel. |
| Comando o Acción | Propósito |
| **tunnel destination** *{ host-name \| ip-address \| ipv6-address}*<br>Ejemplo:<br>Router (config -if) # tunnel destination FD3A:9A29:9C85:1000::2 | Especifica el destino de una interfaz de túnel. |
| Comando o Acción | Propósito |
| **tunnel mode {aurp \| cayman \| dvmrp \| eon \| gre \| gre multipoint \|**<br>**gre ipv6 \| ipip [decapsulate-any] \| ipsec ipv4 \| iptalk \| ipv6 \| ipsec**<br>**ipv6 \| mpls \| nos \| rbscp}**<br>Ejemplo:<br>Router (config-if)# tunnel mode ipsec ipv6 | Establece el modo de encapsulación para la interfaz de túnel.<br>Para Ipsec, solo las palabras clave IPv6 Ipsec son compatibles. |
| Comando o Acción | Propósito |
| **tunnel protection ipsec profile** *name* **[shared]**<br>Ejemplo:<br>Router(config-if)# tunnel protection ipsec profile profile1 | Asocia una interfaz de túnel con un perfil de IPsec. |
| Comando o Acción | Propósito |
| **End**<br>Ejemplo:<br>Router(config-if)# end | Sale del modo de configuración de la interfaz y retorna al modo privilegiado. |

COMANDOS DE CONFIGURACION OSPFv3

| **HABILITANDO OSPF PARA IPv6 EN UNA INTERFAZ** | |
|---|---|
| Comando o Acción | Propósito |
| **enable**<br>Ejemplo:<br>Router> enable | Habilita executar en modo privilegiado |
| Comando o Acción | Propósito |
| **configure terminal**<br>Ejemplo:<br>Router# configure terminal | Ingresa al modo de configuración global |
| Comando o Acción | Propósito |
| **ipv6 unicast-routing**<br>Ejemplo:<br>Router(config)# ipv6 unicast-routing | Habilita el intercambio de datagramas unicast IPv6. |
| Comando o Acción | Propósito |
| **ipv6 cef**<br>Ejemplo:<br>Router(config)# ipv6 cef | Activar Cisco Express Forwarding global en el router. |
| Comando o Acción | Propósito |
| **interface** type number<br>Ejemplo:<br>Router(config)# interface serial 0/0 | Especifica la interface en la que OSPF se va a configurar. |
| Comando o Acción | Propósito |
| **no shutdown**<br>Ejemplo:<br>Router(config-if)# no shutdown | Habilita la interface y empieza el proceso de enrutamiento. |

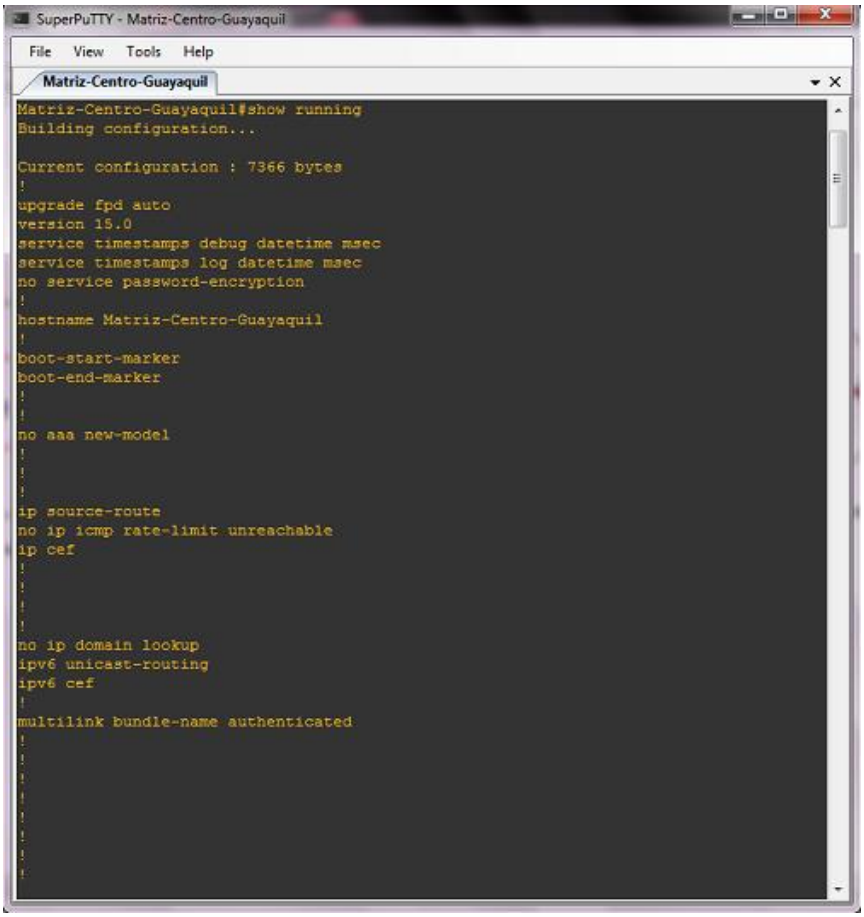
| Comando o Acción | Propósito |
|---|---|
| **ipv6 enable**<br>Ejemplo:<br>Router(config-if)# ipv6 enable | Permite el procesamiento de IPv6 en una interfaz que no se ha configurado con una dirección IPv6 explicita. |
| Comando o Acción | Propósito |
| **ipv6 ospf** *process-id* **area** *area-id*<br>Ejemplo:<br>**ipv6 ospf 1 area 0** | Configura un area en OSPFv3 |
| Comando o Acción | Propósito |
| **ipv6 router ospf** *as-number*<br>Ejemplo:<br>Router(config-if)# ipv6 router ospf 1 | Entra en el modo de configuración del router y crea un proceso de enrutamiento IPv6 OSPF |
| Comando o Acción | Propósito |
| **router-id** *ip-address*<br>Ejemplo:<br>Router(config-router)# router-id 1.1.1.1 | Permite el uso de un ID fijo en un router. |
| Comando o Acción | Propósito |
| **exit**<br>Ejemplo:<br>Router(config-router)# exit | Permite regresar al modo EXEC |

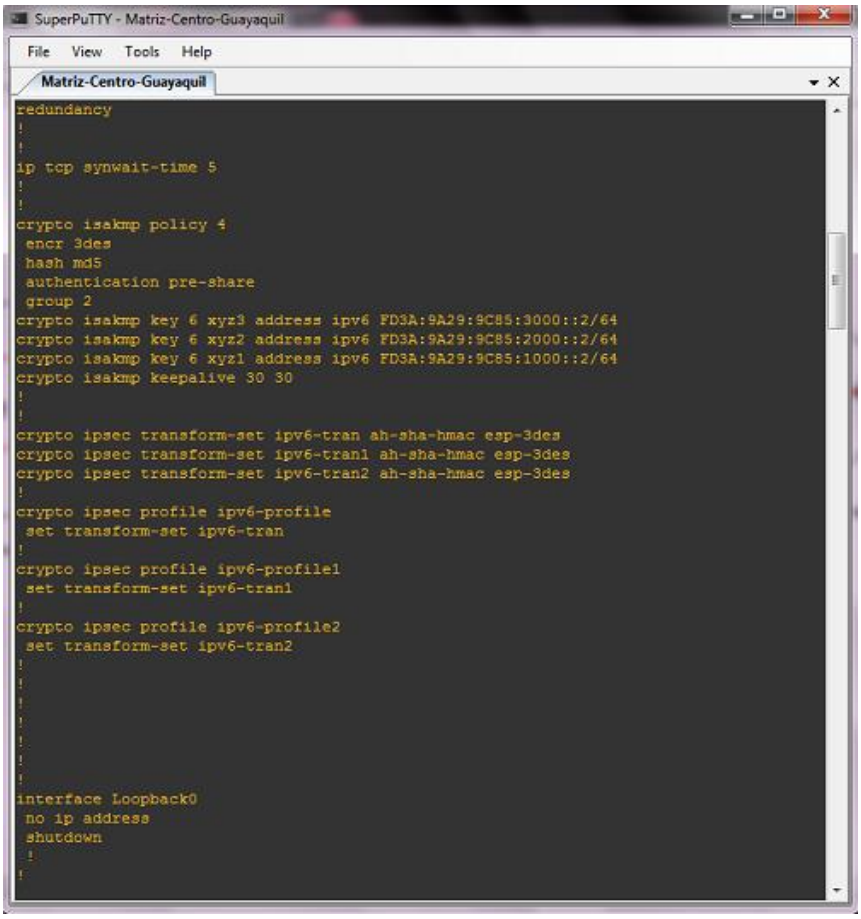
COMANDOS DE CONFIGURACION SNMPv3

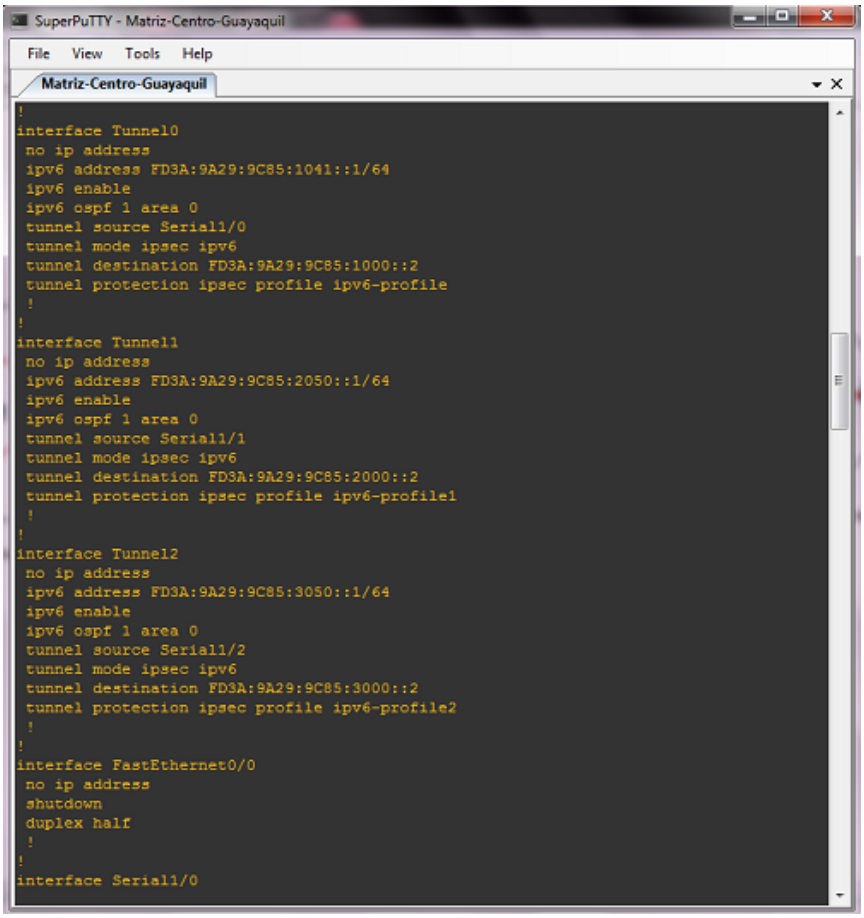
| **HABILITANDO SNMP v3** | |
|---|---|
| Comando o Acción | Propósito |
| **enable**<br>Ejemplo:<br>Router> enable | Habilita executar en modo privilegiado |
| Comando o Acción | Propósito |
| **configure terminal**<br>Ejemplo:<br>Router# configure terminal | Ingresa al modo de configuración global |
| Comando o Acción | Propósito |
| **snmp-server group** *V3Group* **v3 priv read** *V3Read* **write** *V3Write*<br>Ejemplo:<br>Router(config)# snmp-server group **GrupoEspol** v3 priv read **ReadEspol** write **WriteEspol** | Creamos un grupo SNMPv3 y especifica el nivel de seguridad que se va a utilizar. Utilizamos autenticación y privacidad para la comunicación. |
| Comando o Acción | Propósito |
| **snmp-server user** *V3User V3Group* **v3 auth sha** *(contraseña)* **priv 3des** *(contraseña)*<br>Ejemplo:<br>Router(config)# **snmp-server user** UserEspol GrupoEspol **v3 auth sha** kwnxpd **priv 3des** 1971kwn | Creamos un usuario al grupo anterior y asignamos niveles de seguridad y autenticación. |
| Comando o Acción | Propósito |
| **snmp-server view** *V3Read* **iso included**<br>Ejemplo:<br>Router(config)# **snmp-server view** *ReadEspo***l iso included** | View especifican los OIDs que van a poder ser accedidos para escritura o lectura por los usuarios de un grupo específico de SNMPv3. |

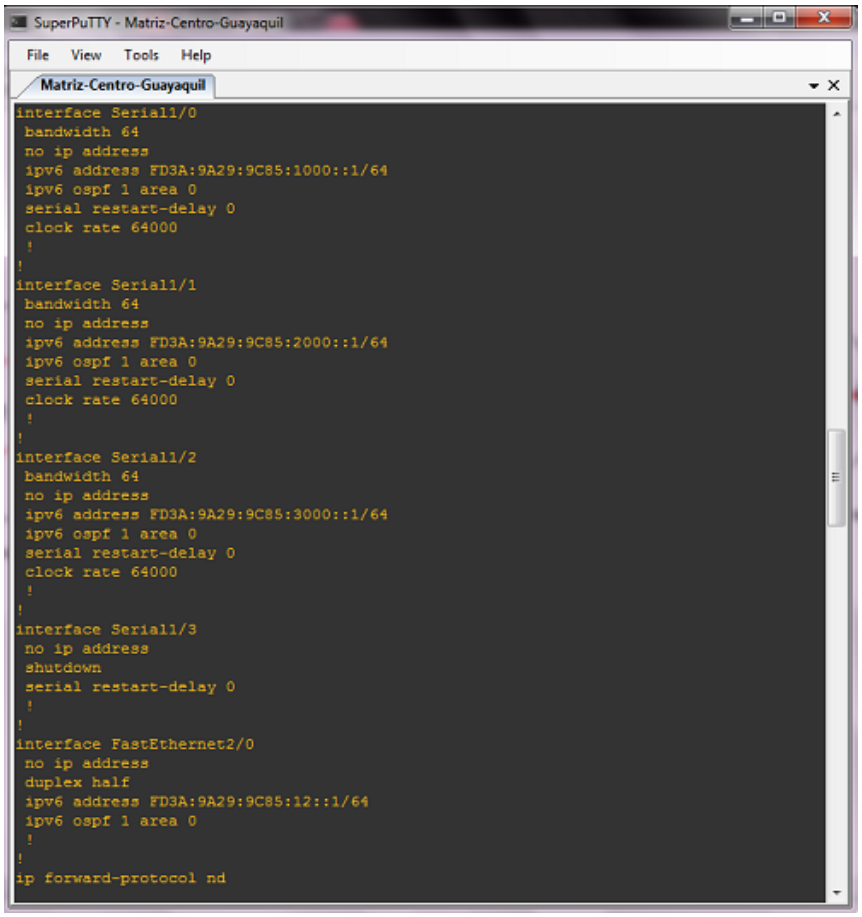
| Comando o Acción | Propósito |
|---|---|
| **snmp-server view** *V3Write* **iso included**<br>Ejemplo:<br>Router(config-if)# **snmp-server view** WriteEspol **iso included** | View especifican los OIDs que van a poder ser accedidos para escritura o lectura por los usuarios de un grupo específico de SNMPv3. |
| Comando o Acción | Propósito |
| **snmp-server host** **.*.*.** **version 3 priv** *V3User*<br>Ejemplo:<br>Router(config-if)# **snmp-server host** FD3A:9A29:9C85:0012::2 **version 3 priv** UserEspol | Defino a que servidor/aplicación son enviados los traps. |
| Comando o Acción | Propósito |
| **snmp-server enable traps**<br>Ejemplo:<br>Router(config-if)# snmp-server enable traps | Se configura el dispositivo para él envió de traps. |
| Comando o Acción | Propósito |
| **exit**<br>Ejemplo:<br>Router# exit | Permite regresar al modo EXEC |

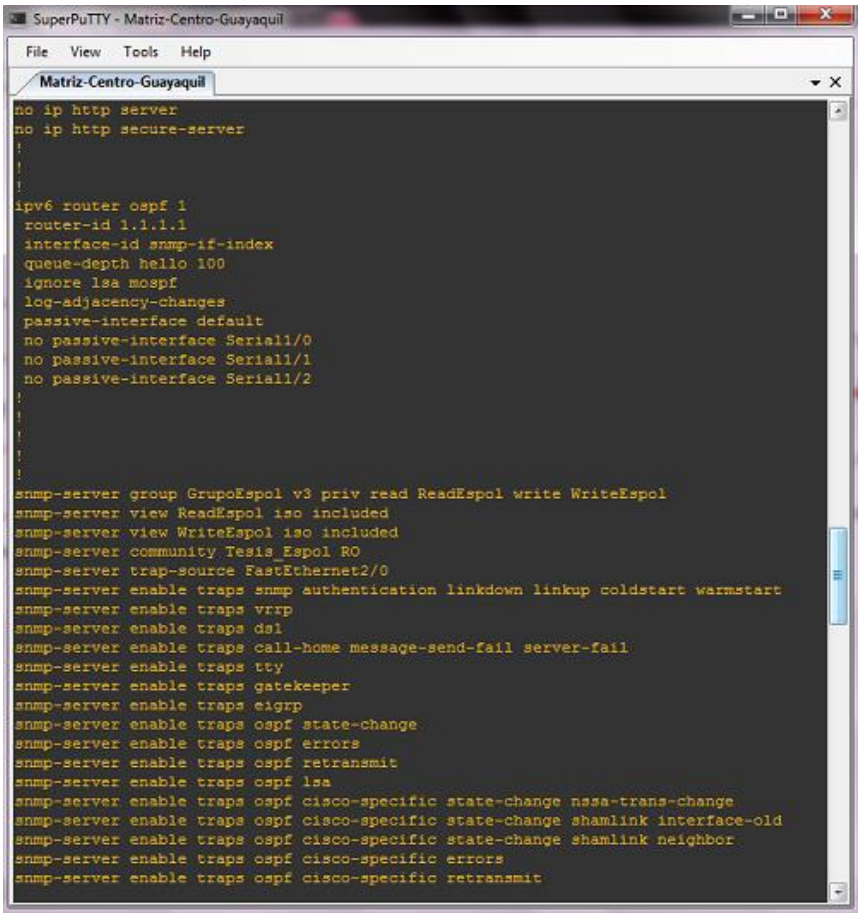
Configuración Activa de Enrutador principal Matriz-Centro-Guayaquil, los demás enrutadores que conforman nuestra red WAN tienen igual configuración, la diferencia está en las direcciones IPv6 asignadas a sus interfaces.

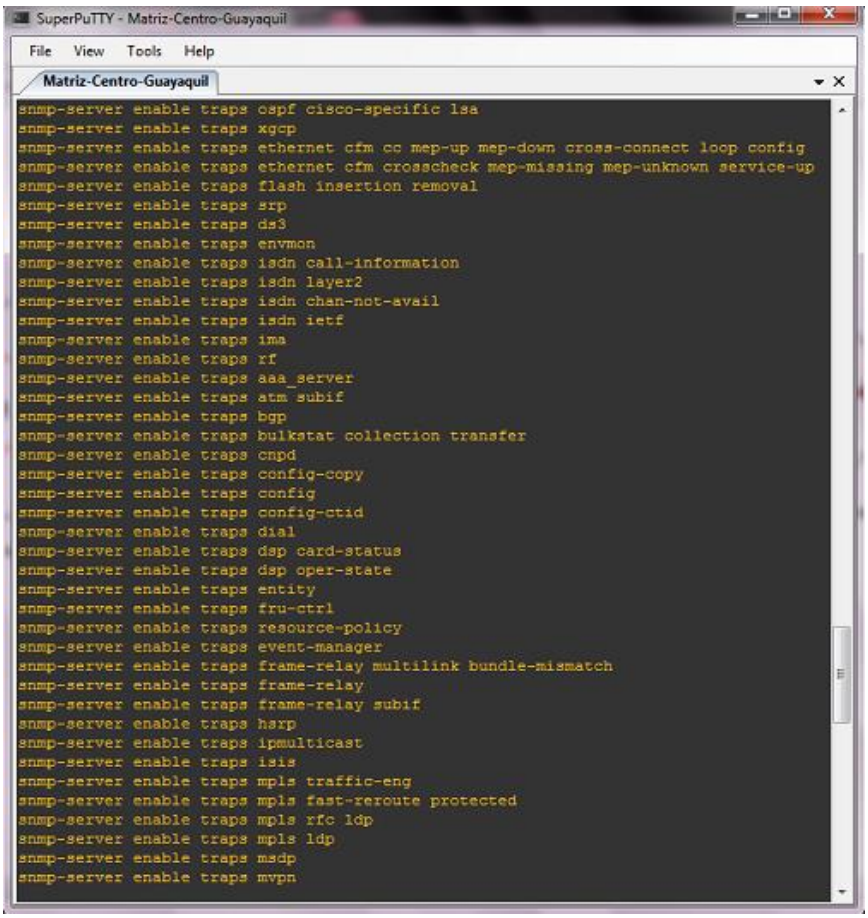


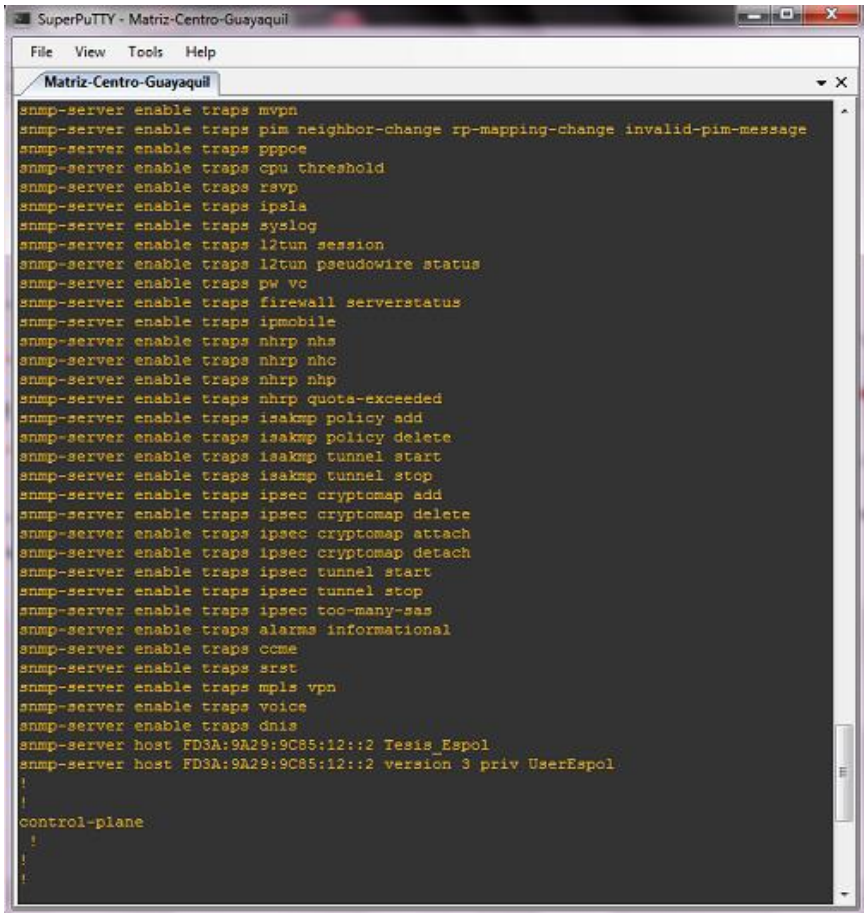

SuperPuTTY - Matriz-Centro-Guayaquil
File View Tools Help
Matriz-Centro-Guayaquil
redundancy
!
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 4
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 xyz3 address ipv6 FD3A:9A29:9C85:3000::2/64
crypto isakmp key 6 xyz2 address ipv6 FD3A:9A29:9C85:2000::2/64
crypto isakmp key 6 xyz1 address ipv6 FD3A:9A29:9C85:1000::2/64
crypto isakmp keepalive 30 30
!
!
crypto ipsec transform-set ipv6-tran ah-sha-hmac esp-3des
crypto ipsec transform-set ipv6-tran1 ah-sha-hmac esp-3des
crypto ipsec transform-set ipv6-tran2 ah-sha-hmac esp-3des
!
crypto ipsec profile ipv6-profile
 set transform-set ipv6-tran
!
crypto ipsec profile ipv6-profile1
 set transform-set ipv6-tran1
!
crypto ipsec profile ipv6-profile2
 set transform-set ipv6-tran2
!
!
!
!
!
!
interface Loopback0
 no ip address
 shutdown
 !
!

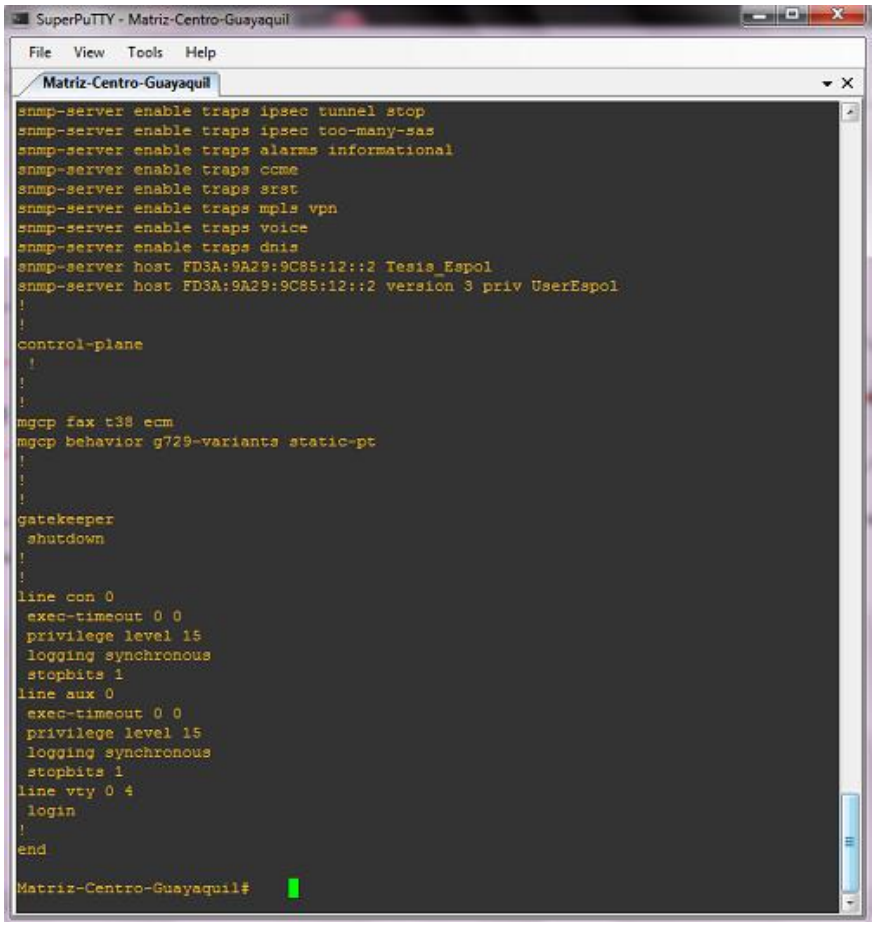

SuperPuTTY - Matriz-Centro-Guayaquil
File View Tools Help
Matriz-Centro-Guayaquil
!
interface Tunnel0
 no ip address
 ipv6 address FD3A:9A29:9C85:1041::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source Serial1/0
 tunnel mode ipsec ipv6
 tunnel destination FD3A:9A29:9C85:1000::2
 tunnel protection ipsec profile ipv6-profile
 !
!
interface Tunnel1
 no ip address
 ipv6 address FD3A:9A29:9C85:2050::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source Serial1/1
 tunnel mode ipsec ipv6
 tunnel destination FD3A:9A29:9C85:2000::2
 tunnel protection ipsec profile ipv6-profile1
 !
!
interface Tunnel2
 no ip address
 ipv6 address FD3A:9A29:9C85:3050::1/64
 ipv6 enable
 ipv6 ospf 1 area 0
 tunnel source Serial1/2
 tunnel mode ipsec ipv6
 tunnel destination FD3A:9A29:9C85:3000::2
 tunnel protection ipsec profile ipv6-profile2
 !
!
interface FastEthernet0/0
 no ip address
 shutdown
 duplex half
 !
!
interface Serial1/0


SuperPuTTY - Matriz-Centro-Guayaquil
File View Tools Help
Matriz-Centro-Guayaquil
interface Serial1/0
 bandwidth 64
 no ip address
 ipv6 address FD3A:9A29:9C85:1000::1/64
 ipv6 ospf 1 area 0
 serial restart-delay 0
 clock rate 64000
 !
!
interface Serial1/1
 bandwidth 64
 no ip address
 ipv6 address FD3A:9A29:9C85:2000::1/64
 ipv6 ospf 1 area 0
 serial restart-delay 0
 clock rate 64000
 !
!
interface Serial1/2
 bandwidth 64
 no ip address
 ipv6 address FD3A:9A29:9C85:3000::1/64
 ipv6 ospf 1 area 0
 serial restart-delay 0
 clock rate 64000
 !
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
 !
!
interface FastEthernet2/0
 no ip address
 duplex half
 ipv6 address FD3A:9A29:9C85:12::1/64
 ipv6 ospf 1 area 0
 !
!
ip forward-protocol nd


SuperPuTTY - Matriz-Centro-Guayaquil
File View Tools Help
Matriz-Centro-Guayaquil
no ip http server
no ip http secure-server
!
!
!
ipv6 router ospf 1
 router-id 1.1.1.1
 interface-id snmp-if-index
 queue-depth hello 100
 ignore lsa mospf
 log-adjacency-changes
 passive-interface default
 no passive-interface Serial1/0
 no passive-interface Serial1/1
 no passive-interface Serial1/2
!
!
!
!
!
snmp-server group GrupoEspol v3 priv read ReadEspol write WriteEspol
snmp-server view ReadEspol iso included
snmp-server view WriteEspol iso included
snmp-server community Tesis_Espol RO
snmp-server trap-source FastEthernet2/0
snmp-server enable traps snmp authentication linkdown linkup coldstart warmstart
snmp-server enable traps vrrp
snmp-server enable traps dsl
snmp-server enable traps call-home message-send-fail server-fail
snmp-server enable traps tty
snmp-server enable traps gatekeeper
snmp-server enable traps eigrp
snmp-server enable traps ospf state-change
snmp-server enable traps ospf errors
snmp-server enable traps ospf retransmit
snmp-server enable traps ospf lsa
snmp-server enable traps ospf cisco-specific state-change nssa-trans-change
snmp-server enable traps ospf cisco-specific state-change shamlink interface-old
snmp-server enable traps ospf cisco-specific state-change shamlink neighbor
snmp-server enable traps ospf cisco-specific errors
snmp-server enable traps ospf cisco-specific retransmit

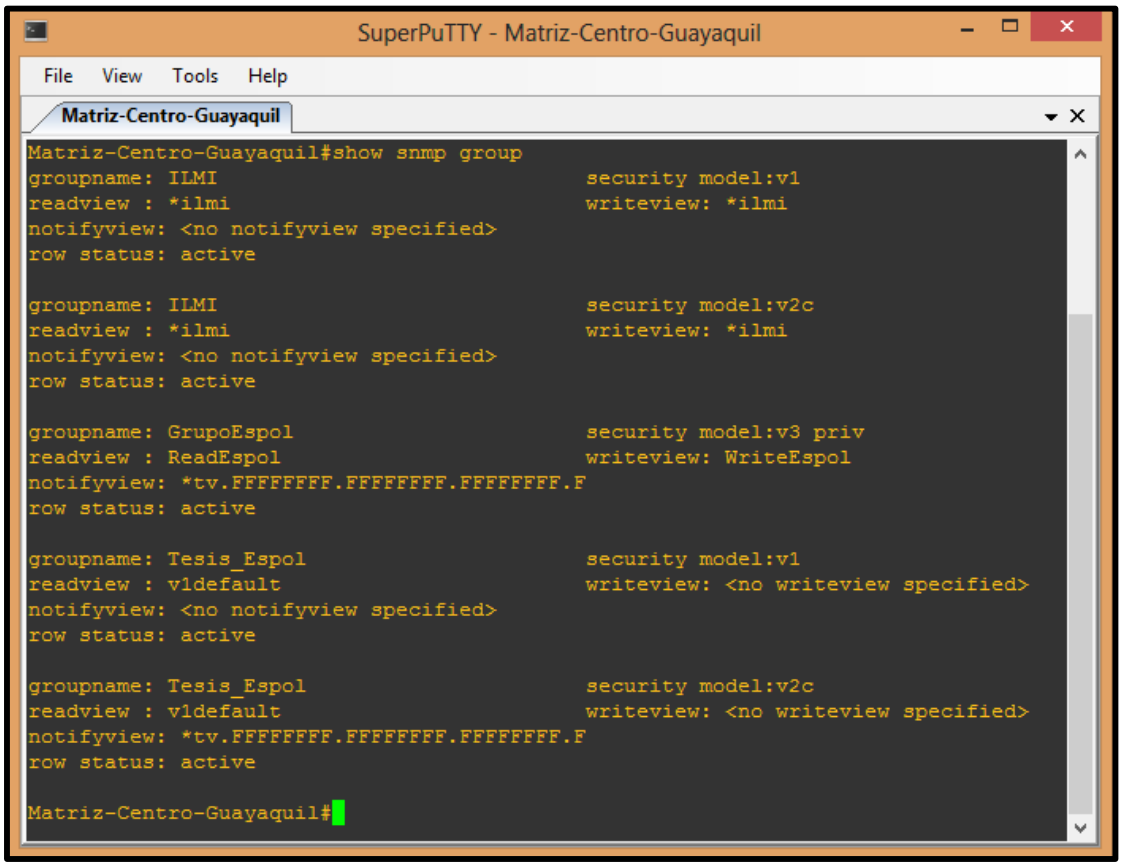

SuperPuTTY - Matriz-Centro-Guayaquil
File View Tools Help
Matriz-Centro-Guayaquil
snmp-server enable traps ospf cisco-specific lsa
snmp-server enable traps xgcp
snmp-server enable traps ethernet cfm cc mep-up mep-down cross-connect loop config
snmp-server enable traps ethernet cfm crosscheck mep-missing mep-unknown service-up
snmp-server enable traps flash insertion removal
snmp-server enable traps srp
snmp-server enable traps ds3
snmp-server enable traps envmon
snmp-server enable traps isdn call-information
snmp-server enable traps isdn layer2
snmp-server enable traps isdn chan-not-avail
snmp-server enable traps isdn ietf
snmp-server enable traps ima
snmp-server enable traps rf
snmp-server enable traps aaa_server
snmp-server enable traps atm subif
snmp-server enable traps bgp
snmp-server enable traps bulkstat collection transfer
snmp-server enable traps cnpd
snmp-server enable traps config-copy
snmp-server enable traps config
snmp-server enable traps config-ctid
snmp-server enable traps dial
snmp-server enable traps dsp card-status
snmp-server enable traps dsp oper-state
snmp-server enable traps entity
snmp-server enable traps fru-ctrl
snmp-server enable traps resource-policy
snmp-server enable traps event-manager
snmp-server enable traps frame-relay multilink bundle-mismatch
snmp-server enable traps frame-relay
snmp-server enable traps frame-relay subif
snmp-server enable traps hsrp
snmp-server enable traps ipmulticast
snmp-server enable traps isis
snmp-server enable traps mpls traffic-eng
snmp-server enable traps mpls fast-reroute protected
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
snmp-server enable traps msdp
snmp-server enable traps mvpn


SuperPuTTY - Matriz-Centro-Guayaquil
File View Tools Help
Matriz-Centro-Guayaquil
snmp-server enable traps mvpn
snmp-server enable traps pim neighbor-change rp-mapping-change invalid-pim-message
snmp-server enable traps pppoe
snmp-server enable traps cpu threshold
snmp-server enable traps rsvp
snmp-server enable traps ipsla
snmp-server enable traps syslog
snmp-server enable traps l2tun session
snmp-server enable traps l2tun pseudowire status
snmp-server enable traps pw vc
snmp-server enable traps firewall serverstatus
snmp-server enable traps ipmobile
snmp-server enable traps nhrp nhs
snmp-server enable traps nhrp nhc
snmp-server enable traps nhrp nhp
snmp-server enable traps nhrp quota-exceeded
snmp-server enable traps isakmp policy add
snmp-server enable traps isakmp policy delete
snmp-server enable traps isakmp tunnel start
snmp-server enable traps isakmp tunnel stop
snmp-server enable traps ipsec cryptomap add
snmp-server enable traps ipsec cryptomap delete
snmp-server enable traps ipsec cryptomap attach
snmp-server enable traps ipsec cryptomap detach
snmp-server enable traps ipsec tunnel start
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps alarms informational
snmp-server enable traps ccme
snmp-server enable traps srst
snmp-server enable traps mpls vpn
snmp-server enable traps voice
snmp-server enable traps dnis
snmp-server host FD3A:9A29:9C85:12::2 Tesis_Espol
snmp-server host FD3A:9A29:9C85:12::2 version 3 priv UserEspol
!
!
control-plane
!
!
!


SuperPuTTY - Matriz-Centro-Guayaquil
File View Tools Help
Matriz-Centro-Guayaquil
snmp-server enable traps ipsec tunnel stop
snmp-server enable traps ipsec too-many-sas
snmp-server enable traps alarms informational
snmp-server enable traps ccme
snmp-server enable traps srst
snmp-server enable traps mpls vpn
snmp-server enable traps voice
snmp-server enable traps dnis
snmp-server host FD3A:9A29:9C85:12::2 Tesis_Espol
snmp-server host FD3A:9A29:9C85:12::2 version 3 priv UserEspol
!
!
control-plane
 !
!
!
mgcp fax t38 ecm
mgcp behavior g729-variants static-pt
!
!
!
gatekeeper
 shutdown
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end
Matriz-Centro-Guayaquil#

Se detalla cómo esta activada la configuración SNMP en sus tres versiones V1, V2c y V3.

El comando Show snmp group nos muestra los grupos y versión del protocolo SNMP activas.



Con el uso del comando Show snmp user, nos muestra el usuario activo y los protocolos de autenticación y protocolos de privacidad utilizados en el Grupo. UserEspol.