Ministerio de Educación Superior
Universidad de Granma

Consejo Nacional de Educación Superior de Ecuador
Universidad Técnica de Cotopaxi

TESIS EN OPCIÓN AL TÍTULO DE INGENIERO INFORMÁTICO Y SISTEMAS COMPUTACIONALES

Título: Análisis y diseño para la instalación del protocolo IPv6 en la red LAN de la Universidad de Granma

Autor: Alex Fernando Aldaz Corrales

Tutor: MSc. Manuel José Linares Alvaro

2007 - 2008

Resumen

Esta investigación, se desarrolló con el propósito de instalar el protocolo IPv6 en la red de la Universidad de Granma de Bayamo, Cuba; documentar los pasos seguidos para ello, de forma que la misma pudiera servir como guía o material de apoyo para trabajos similares en redes de otras entidades y finalmente, ofrecer soluciones a las limitaciones técnicas que habían impedido hasta este momento la instauración de este protocolo en la institución antes mencionada, tales como la falta de soporte por parte de los proveedores.

Para lograr los objetivos señalados, el primer paso consistió en buscar las soluciones a corto plazo mas eficaces para lograr las comunicaciones con protocolo IPv6 entre los dos nodos mas importantes de la red, aún con la carencia de soporte para el protocolo IPv6 por parte de los dos routers que conectan ëstas, esto se logró, creando un túnel de tipo SIT para encapsular el protocolo IPv6 en IPv4, entre los dos servidores – enrutadores con sistema operativo Linux que se hallan en los extremos de las redes de ambos nodos, acto seguido, se llevó a cabo la segmentación de la dirección de red asignada por RedUniv, que permitiera posteriormente, la configuración del protocolo y asignación de direcciones IPv6 fijas a los servidores de la red universitaria, posteriormente se crearon los correspondientes cortafuegos en ambos routers, empleando para ello el IP6Tables, luego, se configuraron los servicios básicos de la red: asignación de direcciones IP sin estado, empleando para ello el Router Advertisement (radvd), DNS, con sus zonas directas e inversas, WWW, FTP, Jabber y enrutamientos multicast.

Adicionalmente, la red interna de los servidores del nodo Bayamo, se conectó a la red externa, pública o global IPv6, empleando también las técnicas de túneles o encapsulación del IPv6, para esto, se creó un túnel, con un servidor público externo (Hurricane Electric: http://tunnelbroker.net), cuyos propósitos, es el enlace a redes externas o hosts con IPv6, para aquellas redes cuyos suministradores no soportan aún este protocolo.

Índice

Introducción

Hoy en día las redes de datos y otros sistemas de comunicación (muy pronto todos los sistemas de comunicación se encontrarán integrados a redes de datos), basan su estructura en el *Protocolo de Internet* (IP). Este protocolo ha ido tomando precedencia en el mundo de las redes de conmutación de paquetes a lo largo de los años, superando a otros protocolos como IPX, Netbeui, entre otros. De hecho, cuando IP fue estandarizado, hace unos veinte años, nadie podía imaginar que se convertiría en lo que es hoy: una arquitectura de amplitud mundial, con un número de usuarios superior al centenar de millones y que crece constantemente de forma exponencial.

IPv4 es la versión del protocolo IP más utilizada actualmente, la cual constituye en estos momentos un Standard. IPv6 es el siguiente paso de IPv4 y, entre otras muchas características, soluciona el problema del limitado número de direcciones IP que existe en el actual protocolo en uso. Por otra parte, a los centros estudio, preferentemente las universidades, les es indispensable la conexión a redes académicas y científicas, cuya base es el IPv6, entre las que se destacan, Internet II y CLARA.

El uso de este protocolo también permitirá prescindir de servidores para la traducción de direcciones de red y Proxys, frecuente solución que se da en las grandes redes a la escasez actual de direcciones IPv4 y garantizará una mayor seguridad.

Por lo antes expuesto, se determinó que el problema de esta investigación lo constituye la no existencia de un protocolo de red en las Universidades Cubanas que contribuya a solucionar la insuficiencia de direcciones IP públicas, se adapte a las necesidades actuales de seguridad, facilite el acceso a redes pertenecientes al sector académico y científico, y que facilite de manera nativa las condiciones técnicas necesarias para la realización de video conferencias, transmisiones de videos, sonidos y multimedios.

Objeto de la investigación: La Red Universitaria de la Universidad de Granma.

Objetivos de la investigación:

General:

- Instalar el protocolo IPv6 en la red LAN de la Universidad de Granma.

Específicos:

- Realizar una búsqueda bibliográfica que condense los aspectos más relevantes relacionados con el protocolo IP, versión 6 que sirva de apoyo para justificar las fases posteriores de esta investigación.
- Buscar alternativas a las soluciones tecnológicas que limitan la implementación de este protocolo en la Universidad de Granma.
- Segmentar la dirección de red IPv6 asignada a la Universidad de Granma por RedUniv, en dependencia de las redes existentes en el campus universitario y las diferentes instancias pertenecientes a la institución.
- Documentar los pasos seguidos durante la instalación del protocolo en la institución, para facilitar la implementación de éste en otras instituciones.
- Formular vías alternativas para la conexión a la red pública IPv6.

Métodos:

La conformación de una teoría que explique el objeto que se estudia presupone modelar dicho objeto, es decir, abstraer un conjunto de características y relaciones de ese objeto, que explique los fenómenos, hechos y procesos que se investigan.

Para realizar estas tareas se han empleado métodos teóricos y empíricos de la investigación científica.

Dentro de los métodos teóricos se utiliza el deductivo directo en el que se obtiene el juicio de una sola premisa, es decir que se llega a una conclusión la implementación del protocolo IPv6 en la red universitaria.

Entre los métodos empíricos usados se puede citar la observación y el análisis de documentos para la recopilación de la información. En la observación el investigador conoce el problema y el objeto de investigación, estudiando su curso natural, sin alteración de las condiciones naturales, es decir que la observación tiene un aspecto contemplativo. La observación configura la base de conocimiento de toda ciencia y, a la vez, es el procedimiento empírico más generalizado de conocimiento. Este fue utilizado para conocer la naturaleza del problema a resolver.

El histórico se usa para determinar la tendencia del objeto de investigación, es decir, como se ha desarrollado el proceso de educación de pregrado hasta la actualidad.

1 Capítulo I. El protocolo IPv6: la solución futura a los problemas y limitaciones de la internet actual.

1.1 Resumen del capítulo.

En este capítulo se hace un análisis comparativo entre los protocolos IPv4 e IPv6, el primero por ser uno de los mas difundidos y utilizados, siendo considerado el Standard actual de Internet y de otras redes, mientras que el segundo, por constituir la nueva versión del protocolo IPv4.

Se analizan las limitaciones del protocolo usado en estos momentos, destacándose las dificultades con su direccionamiento, enrutamientos y seguridad, haciendo hincapié en la manera en que las características del IPv6 contribuirán a solucionar estas limitantes del actual protocolo. Finalmente, se desarrolla un estudio comparativo entre ambos protocolos para demostrar la superioridad de la nueva versión del protocolo IP (IPv6).

1.2 Generalidades sobre redes de ordenadores.

Conceptos básicos.

1.2.1 Redes de Computadoras.

Son numerosos los autores que han enunciado el concepto de redes de computadoras, entre éstos, se puede citar a Naranjo (1997), quien afirma que la definición más precisa de una red es la que se refiere a un sistema de comunicaciones, que propicia la comunicación entre varios usuarios, compartiendo recursos de hardware y datos. Es decir es un sistema de comunicaciones que conecta a varias unidades y que les permite intercambiar información.

En su nivel más elemental, una red consiste de una determinada cantidad de computadoras conectadas de cierta manera para intercambiar información, para lo cual emplean un protocolo de comunicación. Tanenbaum (1996), afirma que una red de computadoras se refiere a una colección interconectada de computadoras autónomas, entendiéndose por computadoras interconectadas a las que son capaces de intercambiar información, la conexión no tiene que ser por medio de un alambre de cobre, puede usarse fibra óptica, microondas y satélites de comunicación, incluso el medio de transmisión puede estar basado en soportes magnéticos.

1.2.1.1 Términos comunes en el lenguaje de redes.

Altes y Serra (2002) mencionan que en informática, un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios.

El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer informacion de modo que otras máquinas puedan utilizar esta.

Según Behrouz (2006), este uso dual puede provocar confusión, por ejemplo, en el caso de un servidor Web, este término podría referirse a la máquina que almacena y maneja los sitios Web, y en este sentido es utilizada por las compañías que ofrecen hosting u hospedaje. Alternativamente, el servidor Web podría referirse al software, como el servidor de http de Apache, que funciona en la máquina y maneja la entrega de los componentes de las páginas Web como respuesta a peticiones de los navegadores de los clientes.

Dicho autor menciona que los clientes son computadoras dedicadas al trabajo de los usuarios, pero que recurren al servidor para obtener sus recursos, ya sean datos, programas o hardware del servidor para correr aplicaciones y obtener resultados localmente.

Lankenau y Garza (2007), alegan que los servidores son computadoras centrales, de gran capacidad, compartidas por las otras computadoras de la red, llamadas clientes o estaciones de trabajo (workstations), ya que reciben el servicio de almacenar, controlar y compartir la información contenida en el servidor. Nótese que el concepto de servidores que ofrecen dichos autores, se refiere a los servidores como computadoras y no al software que brinda el servicio.

1.2.2 Clasificación de las redes de ordenadores.

Si se tiene en cuenta la definición de redes formulada anteriormente, es necesario destacar que este concepto genérico de red incluye varios tipos de ellas, con distintas posibilidades de configuración, por lo que desde un principio surgió la necesidad de establecer clasificaciones que permitieran identificar estructuras de redes concretas. Varios autores coinciden en que las redes pueden clasificarse de acuerdo a la tecnología de transmisión de datos, por el tipo de transferencia de datos que soportan, por su topología, según su tamaño y extensión, o lo que es lo mismo, la magnitud del área que ocupan (García B, 2003; Moreno, 2003).

De acuerdo a la tecnología empleada en la transmisión de datos, nos indica Linares (2007) que las redes se agrupan en redes broadcast y punto a punto. Atendiendo al tipo

de transferencia de datos que soportan, se clasifican en redes de transmisión simple, redes half duplex y redes full duplex.

En lo referente a la topología de las redes, Behrouz (2006) agrupa las redes en aquellas con topologías en forma de árbol, bus, estrella, celular y malla.

Rengifo (2004), indica que además de las ya mencionadas existen otras topologías como son la celular, la topología en trama y las hibridas o irregulares.

Atendiendo al ámbito que abarcan, tradicionalmente se habla de redes de área local (LAN, Local Área Networks) que conectan varias estaciones dentro de la misma institución, redes de área metropolitana (MAN, Metropolitan Área Networks), las cuales superan en extensión a las redes LAN, soliendo abarcar el área de una ciudad, típicas de instituciones que poseen diferentes oficinas repartidas en una misma área metropolitana, pudiendo alcanzar hasta 10 kilómetros de tamaño. Finalmente, las redes de área extensa (WAN Wide Área Networks), que superan los 10 kilómetros, y pueden llegar hasta 10000 kilómetros. La red Universitaria Cubana, RedUniv es un típico ejemplo de redes WAN, la cual se extiende a todo lo largo del territorio cubano, interconectando todas las universidades, algunos centros de investigación y Sedes Universitarias Municipales (SUM).

Geneul (2005) y Moreno (2003), incluyen un nuevo tipo de red en esta clasificación: La red Internet, la autopista de la información, o simplemente, como muchos la llaman, la red.

Podría considerarse la red Internet como una red WAN, pero, es tal su magnitud (se sale de los límites del planeta) y ha sido tan grande el desarrollo alcanzado por ésta en los últimos tiempos, que la misma puede considerarse como un tipo de red, de mayor magnitud aún que las redes WAN, pues abarca prácticamente todo el planeta, equipos de varias clases: desde computadoras hasta aparatos domésticos como neveras, lavadoras, etc., y millones de usuarios.

Black (1999), además de que indica la existencia de las anteriores redes, menciona las Redes Globales GAN (Global Área Network)

1.2.3 Protocolos.

Según Tanenbaum (1996), los protocolos son reglas y procedimientos para comunicarse, o lo que es lo mismo un acuerdo entre las partes que se comunican sobre la forma en que va a proceder esta comunicación.

Dicho autor indica que el uso de las reglas de comunicación o protocolos se aplica de la misma manera al entorno de los ordenadores. Cuando varios ordenadores están en red,

las reglas y procedimientos técnicos que gobiernan su comunicación e interacción se llama un protocolo.

Por lo tanto, Soto (2006), afirma que los protocolos son reglas y procedimientos que se utilizan para las comunicaciones a través de redes a los cuales están sometidos todos los usuarios y equipos.

Este mismo autor menciona que los protocolos de red proporcionan lo que se denomina servicios de enlace. Estos protocolos gestionan información sobre direccionamiento y encaminamiento, comprobación de errores y peticiones de retransmisión. Los protocolos de red también definen reglas para la comunicación en un entorno de red particular como es Ethernet o Token Ring.

1.2.3.1 Ejemplos de protocolos utilizados actualmente.

ICMP (Internet Control Message Protocol o Protocolo de control de mensajes de internet) Son protocolos que se usan para probar Internet (Tanenbaum, 1996).

ARP (Address Resolution Protocol o Protocolo de resolución de direcciones). Es un protocolo de la capa de red, responsable de encontrar la dirección hardware (Ethernet o MAC) que corresponde a una determinada dirección IP (Plumer, 1982).

RARP (Reverse Address Resolution Protocol o Protocolo de resolución de direcciones inverso). Es un protocolo utilizado para resolver la dirección IP a partir de una dirección de hardware dada (como una dirección Ethernet). Todas las tarjetas Ethernet desde el momento en que son fabricadas se les asigna una dirección de ethernet de 48 bits. Una autoridad central le asigna a los fabricantes bloques de direcciones para evitar que las mismas se pudieran repetir. Las tarjetas Ethernet, envían y reciben marcos con base a direcciones Ethernet de 48 bits (Finlayson, Mann, Mogul, y Theimer, 1984).

BOOTP este reemplazó al anterior protocolo (ARP), ya que funciona con paquetes UDP, los cuales se reenvían a través de los routers, eliminando la necesidad de disponer de un servidor BOOTP en cada subred como en el caso anterior y, además, BOOTP ya tiene un conjunto de funciones mayor que permite obtener más información y no sólo la dirección IP (Tanenbaum, 1996).

IPX (Internetwork Packet Exchange o Intercambio de paquetes interred). Protocolo utilizado en las redes Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Actualmente este protocolo esta en desuso y solo se utiliza para juegos en red antiguos (Atkinson, 1998).

NetBEUI (NetBIOS Extended User Interface, en español Interfaz extendida de usuario de NetBIOS), es un protocolo de nivel de red sin encaminamiento y bastante sencillo utilizado

como una de las capas en las primeras redes de Microsoft. NetBIOS sobre NetBEUI es utilizado por muchos sistemas operativos desarrollados en los 1990, como LAN Manager, LAN Server, Windows 3.x, Windows 95 y Windows NT (Soto, 2006).

El Instituto de Ingenieros Eléctricos y Electrónicos, IEEE (802) señala que este protocolo a veces es confundido con NetBIOS, pero NetBIOS es una idea de como un grupo de servicios deben ser dados a las aplicaciones. Con NetBEUI se convierte en un protocolo que implementa estos servicios. NetBEUI puede ser visto como una implementacion de NetBIOS sobre IEEE 802.2 LLC.

La arquitectura TCP/IP esta hoy en día ampliamente difundida, a pesar de ser una arquitectura de facto, en lugar de ser uno de los estándares definidos por la ISO, IICC, etc (Aldo, Gabriel, y Mariano, 2006).

Tanenbaum (1996), coincide también con el autor citado anteriormente, en que la arquitectura TCP/IP es una de las mas difundidas hoy en redes corporativas, institucionales y desde luego, en la red Internet.

1.2.4 Arquitectura TCP/IP.

TCP/IP son las siglas de Protocolo de Control de Transmisión/Protocolo de Internet (Transmission Control Protocol/Internet Protocol), Es un sistema de protocolos que hacen posibles servicios tales como Telnet, FTP, E-mail, www y otros entre ordenadores que no pertenecen a la misma red (Soto, 2006). Mientras que Atkinson (1998) e IETF(1992) indican que TCP/IP es un conjunto de protocolos llamado así por los protocolos que lo conforman, constituyen la base para las comunicaciones de redes locales y estos a su vez están sometidos a estándares por el IETF.

Tanenbaum (1996), menciona que al contrario de lo que ocurre con OSI (open system interconnection, interconexión de sistemas abiertos), el modelo TCP/IP es software, es decir, es un modelo para ser implementado en cualquier tipo de red, el mismo facilita el intercambio de información independientemente de la tecnología y el tipo de subredes a atravesar. Por todo esto, TCP/IP no define una capa física ni de enlace. Este protocolo define solamente tres capas que funcionarán en los niveles superiores a las capas físicas y de enlace para hacerlo así un modelo independiente del hardware en el que se implemente.

Este autor, indica que este modelo posee 4 capas las cuales se muestran en la figura 1.1, y se explican a continuación.

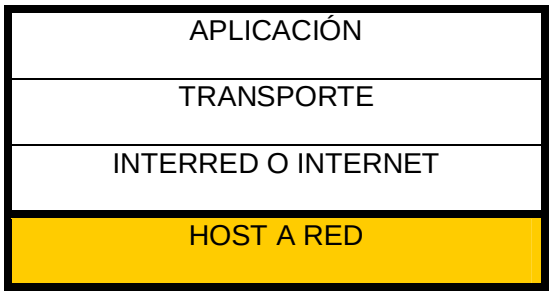

Figura 1.1 Esquema de la Arquitectura TCP/IP

1.2.4.1 Capa de Interred o Internet.

Esta capa es el eje que mantiene unida toda la arquitectura, permite que los nodos inyecten paquetes en cualquier red y los hagan viajar de forma independiente a su destino (que podría estar en una red diferente). El trabajo de esta capa es entregar paquetes IP a donde se supone que deben ir. Aquí la consideración más importante es claramente el ruteo de los paquetes y también evitar la congestión.

1.2.4.2 Capa de transporte.

Esta capa se diseño para permitir que las entidades pares en los nodos de origen y destino, lleven a cabo una conversación. Aquí se definieron los protocolos de extremo a extremo, el primero, TCP (transmisión control protocol, protocolo de control de transmisión) y el UDP (User Datagram Protocol, protocolo de datagrama de usuario).

Las relaciones entre IP, TCP y UDP, se muestran en la figura 1.2 siguiente.

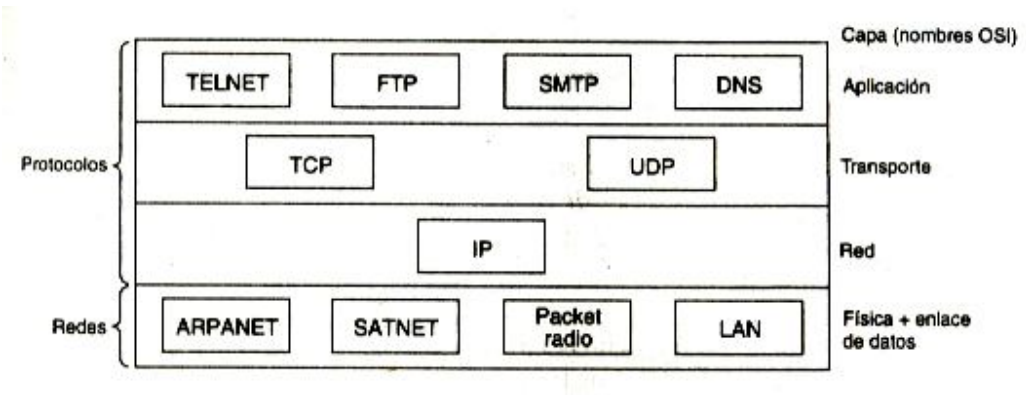

Figura 1.2 Protocolos y redes en el modelo TCP/IP inicial

1.2.4.3 Capa de aplicación.

Encima de la capa de transporte, se halla la capa de aplicación, que contiene los protocolos de alto nivel. Entre los más antiguos están el de terminales virtuales (Telnet), el

de transferencia de archivos (FTP), el de correo electrónico (SMTP), como se muestra en la figura 1.2.

1.2.4.4 Capa de host a red.

Bajo la capa de interred esta un gran vació, fuera de indicar que el nodo se ha de conectar a la red haciendo uso de algún protocolo de modo que pueda enviar por ella paquetes de IP.

Esta investigación se centra principalmente en el estudio del protocolo TCP/IP, perteneciente a la Capa de Red, específicamente en la versión 4 por ser la mas utilizada actualmente y en la versión 6 por ser ésta parte de la solución que brinda esta investigación.

1.3 IP, versión 4 (IPv4).

1.3.1 Historia.

Según Atelin y Dordoigne (2002), el protocolo IP, (Internet Protocol o protocolo de Internet), fue diseñado inicialmente para cubrir las necesidades del Departamento de Defensa de los Estados Unidos (Department of Defense of Unite State, DoD). A finales de la década del 60, el DoD empezó a hacer acuerdos con Universidades de los Estados Unidos y la comunidad de investigación para diseñar estándares y protocolos abiertos para su red conocida como ARPANET. La inicial ARPANET, la primera red de conmutación de paquetes, empezó su operación en 1969 conectando 4 universidades, 3 en el estado de California y la otra en el estado de Utah, los cuales se enlazaron utilizando el protocolo NCP (el predecesor de TCP/IP).

En 1974, estaba listo el diseño de un nuevo conjunto de protocolos para la ARPANET. El nombre oficial para ese conjunto de protocolos fue TCP/IP, el cual fue tomado de los nombres del protocolo de capa de red, Internet Protocol (IP), y de uno de los protocolos de la capa de transporte, Transmission Control Protocol (TCP) (Tanenbaum, 1996).

La versión de IP comúnmente usada es la versión 4 (IPv4), la cual no ha sido substancialmente modificada desde que el RFC 791 fue publicado en 1981. Desde ese momento, IPv4 ha probado ser robusta, fácil de implementar e interoperable, la prueba más real es la red Internet de la actualidad (Atkinson, 1998).

1.3.2 Estado actual.

En la actualidad, IPv4 se usa para muchos propósitos, no sólo se limita a su empleo en la Internet, sino, es utilizado frecuentemente en intranets, redes privadas del tipo MAN y

WAN. En tales entornos, IPv4 ofrece ventajas significativas sobre otros protocolos de red, pues trabaja sobre una gran variedad de hardware y sistemas operativos. De este modo puede crearse fácilmente una red heterogénea usando este protocolo. Dicha red puede contener estaciones Mac, PC compatibles, estaciones Sun, servidores Novell, etc. Todos estos elementos pueden comunicarse usando la misma suite de protocolos TCP/IP (Ureña-Poirier y Martín, 2005).

También es importante señalar, que este protocolo es utilizado en las redes de transmisión de datos de las compañías y distribuidores de servicios de comunicaciones para la comunicación entre las diversas plantas de servicios telefónicos, transmisión de datos, etc.

Atelin y Dordoigne (2002), opinan que el protocolo IPv4, creado hace mas de 20 años, ha probado tener un diseño flexible pero está presentando actualmente algunos inconvenientes, relacionados con el uso de la red por millones de personas en el planeta, lo que implica una exponencial demanda de direcciones IP, provocando en los próximos años el agotamiento de las direcciones IP disponibles, tablas de enrutamiento de gran tamaño, protocolo complicado e ineficiente por un procesamiento lento en los enrutadores, no posee funcionalidad para dar seguridad, pobre atención a los tipos de servicios, además, es complicado para trabajar con IP Móvil.

Cuando se diseñó el actual protocolo de Internet IPv4, no se tuvo en cuenta el crecimiento exponencial que ha experimentado en los últimos diez años. Cada vez hay más usuarios, y el espacio de direcciones que proporciona IPv4 empieza a quedarse pequeño. A la vez se pide nueva funcionalidad extra como seguridad, eficiencia, calidad de servicio, a un protocolo que nunca fue diseñado con esos fines, nunca se creo pensando en una implantación a gran escala, de modo que actualmente los enrutadores, tienen que consumir una considerable cantidad de recursos solo para hacer el mas simple encaminamiento, sin proporcionar ninguna funcionalidad adicional, pero por el momento este protocolo a solucionado algunos inconvenientes (Sedano, 2001).

1.3.3 Características.

Ureña-Poirier y Martín (2005), refieren que entre las principales características del IPv4 si se compara con otros protocolos, se encuentra la de consumir pocos recursos de red, además, de poder ser implementado a un coste mucho menor que otras opciones, este protocolo se integró en la versión 4.2 del sistema operativo UNIX de Berkeley y la inclusión a versiones comerciales de UNIX vino pronto. Así es como TCP/IP se convirtió en el estándar de Internet.

El protocolo IPv4 está diseñado para trabajar sobre cualquier tipo de red, sin tener en cuenta el tipo de medio físico en la transmisión de datos, es por ello, que este protocolo no tiene en cuenta, si la red, en la que se encuentra utiliza como medio de transmisión, cables, fibras ópticas o medios inalámbricos; además está diseñado para enrutar, tiene un grado muy elevado de fiabilidad y es adecuado para redes de varios tamaños o magnitudes.

La información, en una red con protocolo TCP/IP, se transmite en forma de paquetes en la capa de transporte, éstos pueden tener un tamaño de hasta 64 kbytes, pero rara vez llegan a alcanzar éste. Estos paquetes, pueden fragmentarse en paquetes más pequeños, en la medida que atraviesan otras redes, o cuando los datos son entregados a la capa de red, con relación a esto, Hernández (2006), afirma que en el Protocolo de Internet se implementan dos funciones básicas: el direccionamiento y la fragmentación. Cada paquete contendrá información, mas una cabecera que consiste un conjunto de bits encargados de suministrar información de control acerca de los datos que contiene el paquete, si el mismo ha sufrido fragmentaciones, etc.

1.3.3.1 Fragmentación.

La fragmentación de un datagrama según Hernández (2006) Lankenau y Garza (2007), es necesaria cuando éste se ha originado en una red que permite paquetes de tamaño grandes y debe atravesar una red que limita el tamaño de los paquetes, para alcanzar su destino final.

Van-Beijnum (2005), menciona que para ensamblar los fragmentos de un datagrama, el módulo IP combina los datagramas que poseen los mismos valores para los 4 campos siguientes: identificación (identification), fuente (source), destino (destination) y protocolo (protocol). El primer fragmento tendrá el campo de fragment offset en cero y el último fragmento tendrá la bandera de more-fragments fijada a cero.

1.3.3.2 Cabeceras IPv4.

Un datagrama posee dos partes: una cabecera y una parte de texto. La cabecera posee una parte fija de 20 bytes y una parte opcional de longitud variable. El formato de la cabecera se muestra en la figura 1.3. Todos estos datos se transmiten en orden *big endian*, (de izquierda a derecha, en forma secuencial, comenzando por el bit de orden mayor del campo versión). En máquinas little endian, se requiere de conversión por software, tanto para la transmisión como para la recepción (Tanenbaum, 1996).

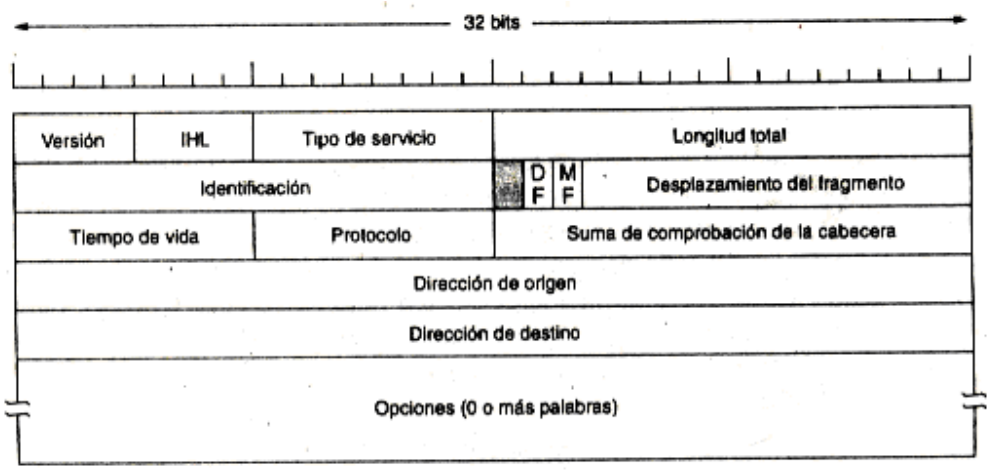

Figura 1.3 La cabecera del Protocolo de Internet

Dicho autor menciona que el *campo versión* (4 bits) lleva el registro de la versión del protocolo al que pertenece el datagrama. Siempre vale lo mismo para el IPv4 (0100).

Dado que el tamaño de la cabecera no es constante, se incluye un campo en esta, el campo *IHL*, de 4 bits, el valor mínimo es de 5, cifra que se aplica cuando no hay opciones, teniendo las cabeceras, en este caso, un tamaño de 20 bytes y el máximo, al ser de 4 bits es de 15, lo que limita la cabecera a 60 bytes, y por tanto, el campo de opciones a 40 bytes.

El campo *tipo de servicio*, indica una serie de parámetros sobre la calidad de servicio deseada durante el tránsito por una red. Existen varias combinaciones de calidad y fiabilidad.

La *longitud total*, 16 bits, incluye todo el datagrama, tanto la cabecera como los datos.

Identificación: Se utilizará, en caso de que el datagrama deba ser fragmentado, para poder distinguir los fragmentos de un datagrama de los de otro. El originador del datagrama debe asegurar un valor único para la pareja origen-destino y el tipo de protocolo durante el tiempo que el datagrama pueda estar activo en la red.

A continuación le sigue un bit sin uso y luego dos campos de un bit: *DF* y *MF*.

DF significa no fragmentar, es una orden para que los enrrutadores no fragmenten el datagrama, porque el destino es incapaz de juntar las piezas de nuevo. *MF* significa más fragmentos, todos los fragmentos, excepto el último tienen establecido este bit a 1, por lo que sirve para indicar cuando han llegado todos los fragmentos de un datagrama.

El *campo desplazamiento del fragmento*, 13 bits, indica la parte del datagrama actual que pertenece al fragmento. Todos los fragmentos, excepto el último del datagrama, deberán tener un número múltiplo de 8, que es la unidad elemental de fragmento, es por ello que

podrá haber un máximo de 8192 fragmentos por cada datagrama, dando una longitud máxima de datagrama de 65536 bytes, uno más que el campo longitud total.

El campo *tiempo de vida* es un contador que sirve para limitar la vida de un paquete, y al ser de 8 bits permitirá un valor máximo de 255, este valor deberá disminuirse en cada salto (paso a través de una pasarela o router), cuando el contador llega a cero, el paquete se descarta y se envía un paquete de aviso al host de origen. Esto evita que los datagramas "vaguen" por la red eternamente, algo que de otra manera podría ocurrir si existen errores de enrutamientos en los routers o pasarelas.

Una vez que la capa de red ha ensamblado un datagrama completo, necesita saber que hacer con él. El *campo de protocolo*, (8 bits), indica el protocolo de la capa de transporte a la que debe entregarse. TCP es una posibilidad, UDP es otra, existen otras más, pero estas son los protocolos mas utilizados.

La *suma de comprobación de la cabecera*, 16 bits, verifica solamente la cabecera, para los fines de este algoritmo, se supone que ésta sea cero cuando llega. Este algoritmo es mas robusto que una suma normal, nótese que la suma de comprobación de la cabecera debe recalcularse en cada salto, pues cuando menos uno de los campos siempre cambia.

La *dirección de origen y dirección de destino* indican el número de red y el número de host que originó un datagrama y al host al que va dirigido un datagrama.

El campo de opciones se diseñó para proporcionar un recurso que permitiera que las versiones subsiguientes del protocolo incluyeran información no presente en el diseño original, para permitir probar a los experimentadores ideas nuevas.

Podrían mencionarse, entre las opciones, la de enrutamiento estricto desde el origen, utilizado para indicar la trayectoria completa a seguir, desde el origen hasta el destino; el enrutamiento libre desde el origen, el cual da una lista de los enrutadores que no deben evitarse pero les permite pasar a través de otros enrutadores en el camino, entre otras.

1.3.3.3 Direccionamiento.

En el protocolo IP las direcciones tienen una longitud de 32 bits, las cuales se agrupan en cuatro octetos de 8 bits cada uno, suelen expresarse de forma decimal y se separan por puntos (ejemplo, 192.168.10.3). Tanenbaum (1996) indica que una dirección IP consta de dos partes: la primera es el número de red, mientras que otra indica la dirección local o número del host. Existen cinco clases de direcciones IP (Figura 1.4): Las direcciones de clase A, en las que el bit de mayor significación, es decir, el bit 0 es igual a 0 y el número de red, llega hasta el bit 7, a partir de éste, es decir, desde el bit 8 hasta el 31, se utiliza para denotar el número de host; las direcciones IP de clase B, en las que el bit cero es

igual a 1 y el bit uno será siempre 0, llegando el número de red, hasta el bit 15, y el número del host, desde el bit 16 hasta el 31. En las direcciones IP de clase C, los bits 0 y 1 valdrán siempre 1, y el bit 2 tomará el valor 0. El número de red en las direcciones de clase C, siempre llegará hasta el bit 23, y el número de host será a partir del bit 24. Las direcciones de clase D son utilizadas para transmisiones multicast y las de clase E agrupan un conjunto de direcciones reservadas para uso futuro.

Existen 126 redes de clase A con 16 millones direcciones cada una, de clase B, 16382 redes con 65535 direcciones y de clase C 2 millones con 256 direcciones.

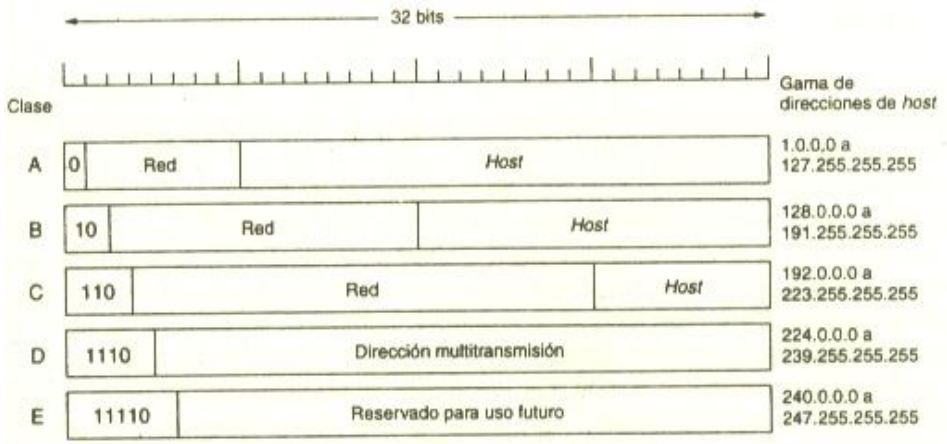

Figura 1.4 Formatos de direcciones IP

Las direcciones que consisten solamente en unos (11111111), se utilizan como dirección Broadcast o multidifusión, o sea la dirección que permite enviar mensajes o datagramas a todas las direcciones IP de una red, por ejemplo, la dirección de clase C 192.168.10.255, todos los paquetes enviados a esta dirección, serán difundidos entre todas las direcciones IP de las máquinas que están en la red 192.168.10.0., desde la maquina 1 hasta la 254.

Por último, todas las direcciones de la forma 127.a.b.c se reservan para pruebas de realimentación. Los paquetes enviados a estas direcciones no se colocan o no llegan a la capa física, sino que se procesan localmente y se tratan como paquetes de entrada.

Existen rangos para asignar direcciones IP a redes y hosts que no están conectados a la red global, por lo tanto no necesitan direcciones IP, reales o públicas, puede ocurrir también que, por cuestiones de seguridad, ciertas instituciones no les asignan direcciones IP públicas a sus redes internas, evitando así que se pueda acceder a estos servidores y hosts desde el exterior o red global, el problema del acceso a la Internet lo resuelven con el uso de servidores proxys y firewalls (corta fuegos). Existen rangos de direcciones IP (tabla 1.1), para el uso de las redes privadas que no tienen un enlace directo a la red global:

Clase	Rango de direcciones
A	10.0.0.0
B	172.16.0.0
C	192.168.0.0
D	244.0.0.0

Tabla 1.1 Rango de direcciones IP

1.3.3.3.1 Máscaras de subred

Las mascaras de subred, se utilizan para definir las subredes, así como para establecer el número de ordenadores que integran una red determinada y la dirección de red establece la dirección base desde la cual empezamos a contar (Tanenbaum, 1996).

Son muy parecidas a las direcciones IP, o sea, formadas por números de 32 bits, los cuales de dividen en 4 octetos como se observa en la tabla 1.2:

Clase	Mascara
A	255.0.0.0
B	255.255.0.0
C	255.255.255.0

Tabla 1.2 Mascaras de subredes

Las máscaras de red o subred, indican la cantidad de computadoras que puede tener una red, por la cantidad de bits a cero que éstas tienen, por ejemplo, si se analiza la red 200.55.149.8, con máscara de clase C 255.255.255.248, podría afirmarse que ésta hace referencia a una red de 8 direcciones, pues la misma, tiene a cero, los tres bits menos significativos de la máscara, y con tres bits se pueden representar 8 direcciones:

Si se expresa la máscara del ejemplo anterior en notación binaria:

11111111.11111111.11111111.11111000

255 255 255 248

Quedan, a cero, los tres últimos bits o bits menos significativos del último octeto y con éstos se pueden representar ocho direcciones: 200.55.149.8, 200.55.149.9, 200.55.149.10, 200.55.149.11, 200.55.149.12, 200.55.149.13, 200.55.149.14 y 200.55.149.15.

Las mascaras de red también se pueden expresar por la cantidad de bits que tengan puestos a uno, por ejemplo es lo mismo decir 255.255.255.248 que 29, por lo tanto, la forma correcta de representar este número de red sería:

200.55.149.8/255.255.255.248 o 200.55.149.8/29

Es importante destacar que en toda red con arquitectura TCP/IP, se utilizarán siempre dos de las direcciones existentes para designar la dirección o número de red, y la dirección de broadcast, por lo tanto, en el ejemplo que se está tratando, se tomaría como número de red, la primera dirección existente: 200.55.149.8 y como dirección de broadcast, la última, es decir, la 200.55.149.15. Nótese que entonces en todas las redes TCP/IP, siempre será necesario prescindir de dos direcciones, la primera, y la última, por lo que a la cantidad de direcciones que indica la máscara, hay que restarle dos para saber la cantidad máxima exacta de hosts que podría tener dicha red.

1.3.4 Nuevos servicios que ofrecen actualmente las redes globales con protocolo TCP/IP versión 4.

Según Villa (2004), entre los servicios que actualmente ofrecen redes globales, como la Internet, se destacan:

Telemedicina Inalámbrica para realizar teleconsultas, acceso a especialistas e información especializada aún en regiones intrincadas, monitoreo remoto de los pacientes (signos vitales, etc.). En la Telemática Automotor también muchos personas la utilizan para solicitud de asistencia médica en el camino, ubicación de servicios de mantenimiento (combustible, aire, etc.), solicitud de asistencia técnica en el camino, localización de Restaurantes y hoteles, acceso a mapas, servicios de entretenimiento. En el mundo comercial, se esta empleando para el monitoreo de existencias de productos, realización de ofertas, reservas de mercancías y ventas, Servicios de video bajo demanda, Reportes para negocios (Ej: congestión de tránsito, información de vuelos, etc.).

Un servicio que evoluciona actualmente es IP Móvil de 3ra Generación (3G). Según Villa (2004), estos son nombrados voz/fax, Navegación web de alta velocidad, videoconferencia, difusión de televisión, Operación IP completa sobre redes de 3ra Generación, incluyendo Voz sobre IP, Velocidades: 144 kbps o mayores en condición de

alta movilidad (vehículos), 384 kbps (movilidad peatonal), 2 Mbps o mayores para tráfico dentro de locales.

El Grupo Gartner (2006), estimó que el mercado electroinformático creció de $2.9 Billones de dólares en el año 2000 a $7.9 Billones en el 2004.

Según este grupo, los nuevos servicios, a los que se pueden acceder utilizando las redes actuales (basadas fundamentalmente en el protocolo IPv4), encuentran grandes aplicaciones, entre las que se destacan, el acceso seguro (inalámbrico) a correo electrónico, comunicaciones integradas: Internet, Mensajes SMS, telefonía, acceso a redes corporativas, calendarios y manejo de documentos corporativos. También señalan, entre las más destacadas tendencias actuales, la manipulación de contenidos (e-books), la sincronización de contenidos con PCs, grabación y reconocimiento de voz, cámaras, reproductores de MP3, juegos, entre otros.

La proliferación y auge alcanzado actualmente en las redes domésticas, y su conexión a las redes globales, no puede dejarse de mencionar entre las tendencias actuales relacionadas con el desarrollo de las redes en los últimos tiempos.

Villa (2004), menciona que una red doméstica se define como una colección de elementos que procesa, gestiona, transporta y almacena información, de manera tal que permita la integración de múltiples dispositivos de cómputo, control, monitoreo y comunicaciones en la casa.

Este autor, era del criterio en el año 2004, que para el 2006, 23 millones de casas tendrían redes (actualmente se estiman unos 6 millones con estas facilidades) y se espera, que para este mismo año, estarán en uso mas de 220 millones de dispositivos de entretenimiento con capacidad de conectarse a redes (no se incluyen computadoras en el dato). El mercado actual se estima en 28 millones.

Hasta aquí, se pueden percibir fácilmente, las dificultades que de manera inevitable, se están presentando en la red global Internet, por utilizar la misma un protocolo diseñado hace unos treinta años, y con fines mucho menos abarcadores que los actuales, ejemplo, en muchas ocasiones hay embotellamientos en los grandes routers, excesiva cantidad de reglas de ruteo, poca seguridad, pocas direcciones IP disponibles, etc.; con relación a esto, Cambronero (2001), asevera que el crecimiento masivo de usuarios comerciales, nuevos tipos de tráfico (multimedia), redes de banda ancha, escasez de direcciones y explosión del tamaño de tablas de encaminamiento; constituyen los problemas más acuciantes que ha presentado el protocolo IPv4 de la red Internet en los últimos tiempos.

Hernández (2006), alega que existen otros factores que limitan la versión del protocolo usado actualmente, y estimulan al desarrollo e implementacion de la nueva versión del IP:

- Necesidad de establecimiento de verdadera Comunicación “Peer to Peer”.
- Compartir contenidos (Ej: Kazaa, Gnutella, etc).
- Procesamiento de datos distribuidos (Ej:SETI@home, Fightaids@home).
- Relaciones personales (Ej: Microsoft Threedegrees).
- Voz sobre IP “Peer to Peer” (Ej: Skype).
- Juegos “Peer to Peer”.
- Seguridad en las comunicaciones “Peer to Peer”.
- Comunicaciones con Calidad de Servicio (QoS).
- Dispositivos Inteligentes con identificador de Radio-Frecuencia (RFID).

1.3.5 Limitaciones actuales del IPv4.

El IPv4, según McPherson y Halabi (2002), posee un espacio de direcciones de 32 bits que permite direccionar 4 Billones de dispositivos (Teóricamente), 250 Millones de dispositivos (Estimado Práctico), este autor, en estudios investigativos, ha determinado que el espacio de direcciones disponibles puede agotarse entre el 2005 y el 2011 (Figura 1.5).

Asi mismo, dicho autor opina que en estos momentos la tecnología esta en auge y el protocolo IPv4 ya esta quedando obsoleto y hay que buscar una alternativa para proveer nuevos servicios de la red para un futuro cercano.

La red global evoluciona cada día, a grandes pasos desde los primeros momentos de su creación, según McPherson y Halabi (2002), desde 1990 hasta 1993 se mantuvo normalmente dicha red y desde 1994 hasta el 2004 se ha incrementado exponencialmente su uso.

Por todas las limitaciones expuestas anteriormente, ha surgido la necesidad de implementar el IPv6, es decir, la versión 6 del actual protocolo IP, versión 4, solucionándose en un futuro cercano, y de manera gradual, las dificultades que hasta aquí han sido tratadas.

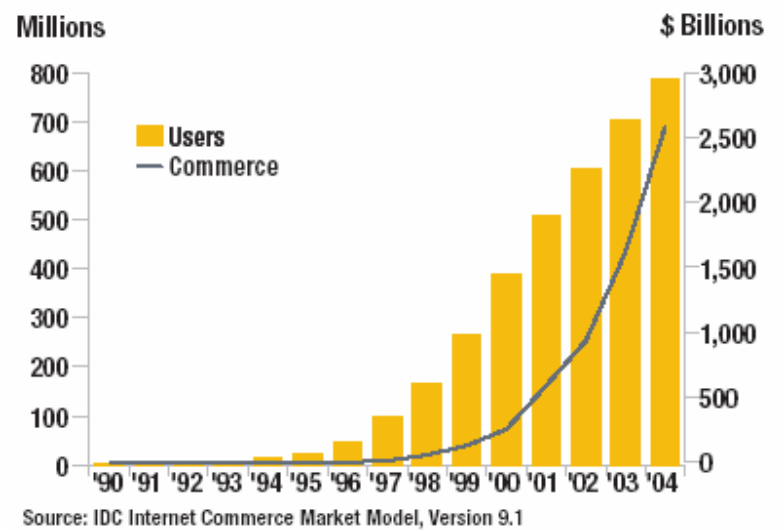

Figura 1.5 Crecimiento exponencial de la red global, según McPherson y Halabi (2002)

1.4 Solución IPv6.

Hernández (2006), indica que para empresas, redes domésticas, industria de juegos, equipos de consumo, computadoras domésticas, proveedores de Servicio (ISP), instituciones gubernamentales, militares, empresas y sectores productivos, desarrolladores de software, universidades, centros académicos e instituciones de Investigación, IPv6 es la única manera de garantizar el crecimiento sostenido de Internet en los próximos años. Hay un gran esfuerzo mundial dedicado al desarrollo y transición a este protocolo, de hecho, ya puede considerarse que el mismo presenta un desarrollo estable y maduro, aún cuando continúan los trabajos en muchas áreas. IPv4 e IPv6 deben coexistir por algún tiempo.

1.5 IP, versión 6 (IPv6).

1.5.1 Historia.

En 1992 aparecen propuestas en la red global Internet por parte del, Engineering Task Force (IETF), (Grupo de Trabajo en Ingeniería de Internet), para elaborar una nueva versión del protocolo IP que mejorará las prestaciones del existente IP versión 4. En 1998 se publica la versión 6 del Protocolo IP (Deering, 1998).

Los mencionados autores exponen que a finales de 1993 se formó el área IPng (IP next generation o la próxima generación IP) para investigar las diferentes propuestas. Después de resolver algunos problemas, se realizó una recomendación del protocolo que incluye una cabecera más simple, con una estructura de direccionamiento jerárquica

suficientemente grande para cumplir con los requerimientos del Internet en el futuro. El protocolo también incluye autentificación a nivel de paquetes, encriptación y auto-configuración. El nuevo diseño cambia la manera en que las opciones de la cabecera IP son codificadas, dándole una mayor flexibilidad para introducir nuevas opciones en el futuro; además, incluye la facilidad de etiquetar flujos de tráfico. A este nuevo protocolo se le ha llamado IPv6.

IPv5 es la versión 5 del Protocolo IP (Internet Protocol), definida como tal en el año 1979 y que no transcendió más allá del ámbito experimental. Nunca se llegó a utilizar como una versión del Protocolo de Internet. La versión número "5" en la cabecera de IP fue asignada para identificar paquetes que llevaban un protocolo experimental, que no era IP, sino ST. ST nunca fue extensamente usado y como la versión número 5 ya estaba asignada, la nueva versión del protocolo IP tuvo que quedarse con el identificador siguiente, el 6 (IPv6). ST está descrito en el RFC 1819 (NA, 2007b).

En 1998-2000 aparecen prototipos IPv6 y se inician eventos de interoperabilidad y redes piloto académicas, se identifican varios métodos técnicos de transición IPV4 a IPV6 (Van-Beijnum, 2005).

El protocolo de Internet versión 6 según Villa (2004), es el mas reciente desarrollo del protocolo IP. Este novedoso protocolo es consecuente con las tecnologías desarrolladas en base al protocolo IPv4, reelaboradas según nuevas filosofías y con el principal objetivo de resolver eficientemente las limitaciones nativas de IPv4 (Van-Beijnum, 2005).

1.5.2 Características más notables del nuevo protocolo.

IPv6 entre muchas características, soluciona el problema de direccionamiento, puesto que a diferencia de su protocolo precedente, que utilizan direcciones de 32 bits (lo que permite un máximo de 4.294.967.296 direcciones disponibles), las de IPv6 están formadas por números de 128 bits, lo que conduce a una cantidad de direcciones utilizables mucho mayor $3.402823669 \times 10^{38}$, o sea alrededor de mil sixtillones. Esto conduce a que desaparezcan los problemas de direccionamiento del IPv4 actual, permitiendo entonces prescindir de técnicas como el NAT para proporcionar conectividad a todos los ordenadores o dispositivos de una red que no cuenten con la cantidad de direcciones IP públicas necesarias. Por tanto, todos los dispositivos actuales o futuros: ordenadores, PDAs, teléfonos GPRS o UMTS, equipos domésticos, entre otros; podrán tener conectividad completa a Internet (Hernández, 2006).

Este autor no menciona que con esta cantidad de direcciones se puede prescindir también del uso de proxys, pues alcanzarán las direcciones IP para todas las estaciones de trabajo de prácticamente, todas las redes de la tierra.

Con el IPv6, al solucionarse la disponibilidad de direcciones, se facilita que los procesos de auto configuración sean mas simples, y esto implica un menor esfuerzo de administración en la configuración de estaciones de trabajo y usuarios corporativos, además, brinda facilidades para el correcto desempeño de IP Móvil, simplifica la construcción de redes domésticas, mejora la seguridad de la red, pues incluye Ipsec de manera obligatoria, lo cual permite garantizar seguridad en la conexión. Al poseer una estructura simplificada en las cabeceras de los paquetes IP, los enrutamientos se hacen más fáciles de procesar, contribuyendo esto, a mejorar la velocidad de procesamiento de los enrutadores (Van-Beijnum, 2005).

Este protocolo, se caracteriza también por poseer mejor soporte al tráfico multimedia en tiempo real que su predecesor IPv4, el multicast es parte nativa del protocolo, y está dotado de mecanismos de transición gradual de IPv4 a IPv6 (Alcantara, 2003).

Senso (1996), indica que la estructura de la cabecera en IPv6 es más simple, con lo que se consigue mejorar el rendimiento de los routers. La existencia de cabeceras de extensión de autentificación, facilita procesos de encriptación de seguridad, permitiendo garantizar la integridad e identidad del paquete. Esto proporciona una notable mejoría en cuestiones de seguridad en relación con el anterior protocolo.

Este mismo autor, señala que el campo de la cabecera "identificador de flujos", el cual posee una longitud de 24 bits, favorecerá la adición entre datagramas de una misma conexión; el campo límite, mejora la rapidez de la transmisión fijando el número máximo de nodos que debe atravesar el datagrama. En el protocolo IPv6, tanto la fragmentación como el ensamblado de paquetes los realizan los sistemas finales, lo que desahoga al router de trabajo. En IPv4 la unidad máxima de transmisión de un enlace con otro es de 64 kbytes, mientras que el mínimo permitido por la nueva versión es 576 kbytes.

Además este autor alega que una de las cualidades más destacadas del nuevo protocolo es la transformación que sufren algunos mecanismos, incluyendo sistemas que podríamos denominar plug and play (enchufar y listo), ya que permite la configuración y conexión automática de equipos a la red.

Otro de los aspectos que caracteriza a este protocolo, menciona Hernández (2006), es que la seguridad de la red, más conocido como IPsec, forma parte integral o nativa del protocolo; en IPv4 el IPsec es opcional.

De acuerdo a las normas de petición de comentarios (Atkinson, 1998), RFC (Request for comments) 2401 y 2411, uno de los grandes problemas propios de la Internet actual, radica en la falta de seguridad de su diseño base. Este es el motivo por el que han tenido que desarrollarse, protocolos seguros como el SSH o SSL, protocolos a nivel de aplicación que añaden una capa de seguridad a las conexiones que pasan a través suyo. IPv6 incluye IPsec, que permite autenticación y encriptación del propio protocolo base, de forma que todas las aplicaciones se pueden beneficiar de ello (Van-Beijnum, 2005).

Es necesario comentar que en este protocolo hay una mayor automatización de procesos, tales como la asignación de información del DNS cuando se asignan las direcciones IP, por ello, no es necesario definir cual será la dirección del servidor de nombres de dominio cuando se asignan direcciones IP, ya sea con o sin estado.

La movilidad se está volviendo una característica importante y crítica en las redes de hoy. Soporte mejorado para IP Móvil es añadido como una nueva característica; en IPv6, cada nodo puede utilizar la movilidad como lo necesite. Las cabeceras de Routing en IPv6 hace que la movilidad sea más eficiente para el usuario final que en IPv4.

En los últimos años ha venido desarrollándose toda una nueva red global, que se ha denominado Internet II, en ésta se ha logrado prevalecer el carácter científico, académico e investigativo, sobre el comercial de la Internet actual. Esta nueva Internet basa sus comunicaciones en el protocolo IPv6. Entre estas redes se destaca, Euro6IX, cuya finalidad es el soporte para lograr una rápida introducción de IPv6 en Europa (Palet, 2003) y la red CLARA: Cooperación Latino Americana de Redes Avanzadas, en la que ya se encuentran Argentina, Brasil, Chile, Colombia, Ecuador, El Salvador, Guatemala, México, Panamá, Perú, Uruguay y Venezuela.

Actualmente el Ministerio de Educación Superior de Cuba tiene entre sus proyectos, el de integrar a las Universidades Cubanas a esta importante red académica latino americana. Las Universidades Cubanas según Hernández (2006), no pueden quedarse a la saga en lo que respecta al dominio, manejo e instalación del protocolo IPv6 en sus redes de cómputo, son varias las causas que hacen necesario esto, en primer término, se solucionarían todo el conjunto de dificultades existentes derivadas del protocolo usado actualmente, además de ser esto una premisa básica para la futura conexión a redes globales avanzadas académicas.

Con el IPv6 se consigue una simplificación en la cabecera, que contiene solamente 8 campos frente a los 13 del IPv4. Este cambio permite a los routers procesar los paquetes mucho más rápido que con antiguas versiones, mejorando así el rendimiento.

1.5.2.1 Estructura de las cabeceras en IPv6.

La cabecera de un paquete IPv6 se muestra en la figura 1.6. Puede apreciarse, si se compara con las cabeceras IPv4, que éstas son sorprendentemente mas sencillas, Peralta (2002); además la funcionalidad del protocolo IPv6 es mucho mayor. La cabecera de un paquete IPv4 es variable, por lo que necesita un campo de tamaño o lenght. Sin embargo, para simplificar el trabajo de los routers, IPv6 utiliza un tamaño de cabecera fijo de 40 bytes, que componen un total de ocho campos.

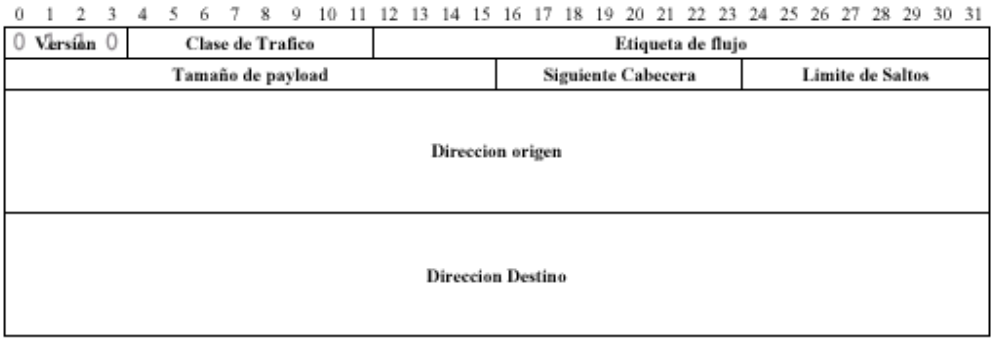

Figura 1.6. Estructura de las cabeceras en los paquetes IPv6

A continuación se explica la función de los diferentes campos, según Peralta (2002).

Versión: (4 bits), sirve para indicar la versión del protocolo.

*Clase de trafico o Traffic Class:***(**8 bits) Este campo es usado por nodos o ruteadores para identificar y distinguir entre diferentes clases o prioridades de los paquetes de IPv6.

Etiqueta de flujo o Flow Label:(20 bits) Se utiliza para etiquetar secuencias de paquetes a los que se debe dar un tratamiento especial por parte de los ruteadores IPv6, como aquellos servicios a tiempo real o aquellos paquetes que no cuentan con la calidad de servicio definida por defecto. Gracias a este campo un ruteador no tiene la necesidad de hacer una revisión profunda del paquete para identificar el flujo, porque esta información está disponible en la cabecera. El campo de etiqueta de flujo permite a las aplicaciones del sistema final diferenciar fácilmente el tráfico en la capa de red, proveyendo más fácilmente QoS para paquetes que han sido encriptados por IPsec.

Tamaño o Payload Length: **(**16 bits) Este campo indica la longitud de la carga útil del paquete de IPv6, es decir, describe el tamaño en octetos de la sección de datos del paquete. Al ser este campo de 16 bits, se puede usar paquetes de hasta más de 64000 bytes.

Siguiente cabecera o Next Header: **(**8 bits) Identifica el tipo de cabecera que sigue inmediatamente después de la cabecera de IPv6, utiliza una manera diferente de manejar información opcional en la cabecera. Define cabeceras de extensión que forman una cadena de estas unidas por el campo “siguiente cabecera”, que se encuentra presente en cada una de ellas. Este mecanismo provee una mayor eficiencia en el procesamiento de cabeceras de extensión, habilita una tasa de envío más rápida y deja al router con menos trabajo de procesamiento por paquete.

Limite de saltos o Hop Limit: **(**8 bits) El valor de este campo se decrementa en uno cada vez que el paquete cruza un nodo. El paquete es descartado si el valor de este campo llega a cero. Debido a que no existe campo de Checksum en la cabecera de IPv6, el router puede decrementar el valor de este campo sin la necesidad de recalcular el Checksum, lo que ahorra recursos de procesamiento. Este campo es similar al campo tiempo de vida en caso del protocolo IPv4.

Dirección origen o Source Address: **(**128 bits) Es la dirección del transmisor del paquete.

Dirección destino o Destination Address: **(**128 bits) Es la dirección del destinatario del paquete.

1.5.2.2 Cabeceras de extensión en IPv6.

A diferencia de IPv4, en IPv6, la información opcional de capa Internet se codifica en cabeceras separadas (Figuras 1.7 y 1.8). Hay un número pequeño de tales cabeceras, cada una identificada por un valor distinto en el campo Next Header (Peralta, 2002).

Figura 1.7 Cabecera IPv6 básica y datos

Figura 1.8 Cabecera IPv6 básica, fragmento y datos

Cuando se usa más de una cabecera de extensión en un mismo paquete, el anterior autor recomienda que esas cabeceras aparezcan en el siguiente orden:

- Cabecera IPv6.
- Cabecera Hop-by-Hop Options.
- Cabecera Destination Options.
- Cabecera Routing.
- Cabecera Fragment.
- Cabecera Authentication.
- Cabecera Encapsulating Security Payload.
- Cabecera Destination Options.
- Cabeceras de capas superiores.

IPv6 soporta varios tipos de direcciones IP y bloques de direcciones más grandes para el uso de ruteo multicast (Deering, 1998).

1.5.2.3 Direccionamiento.

El esquema de direccionamiento de IPv6 ha sido diseñado para proveer compatibilidad he interoperabilidad con la arquitectura existente de IPv4, permitiendo la coexistencia de redes con ambos protocolos. IPv6 no solo resuelve el problema de escasez de direcciones de IPv4, sino que además mejora algunas de sus características (Villa, 2004).

1.5.2.3.1 Formato de las direcciones en IPv6.

IPv6 se basa en direcciones de 128 bits, y se representan, dividiéndolas y separándolas en grupos de 16 bits, éstos se separan utilizando el símbolo dos puntos y se representan con notación hexadecimal. Por ejemplo, aquí se muestra dos direcciones válidas de IPv6.

2031:0000:130f:0000:0000:09C0:876a:130B.

2001:0b00:f80b:0001:0000:0000:0000:0001

Adicionalmente, para hacer que las direcciones IPv6 sean más cortas y fáciles de representar, IPv6 utiliza las siguientes convenciones:

Ceros seguidos en la dirección pueden ser representados de una manera corta. Por ejemplo:

2031:0000:130f:0000:0000:09C0:876a:130B = 2031:0:130f:0:0:09C0:876a:130B.

2001:0b00:f80b:0001:0000:0000:0000:0001 = 2001:b00:f80b:1:0:0:0:1

Un par de dos puntos (::) representan campos sucesivos de ceros. Sin embargo, un par de dos puntos solo son permitidos en una dirección de IPv6 válida. Por ejemplo:

2031:0:130f:0:0:09C0:876a:130B = 2031:0:130f::9C0:876a:130B.
2001:0b00:f80b:0001:0000:0000:0000:0001 = 2001:b00:f80b:1::1

Los bits más significativos, es decir, los que se sitúan hacia la izquierda de la dirección IP, representan el identificador de red, y serán distinguidos en base a un número que indicará la longitud de este prefijo.

Existen tres tipos de direcciones IPv6 según (Peralta, 2002):

Unicast: Es una dirección para una sola interface. Un paquete que es enviado a una dirección unicast se entrega solo a la interface que es identificada por esa dirección.

Anycast: Es una dirección para un grupo de interfaces que por lo general pertenecen a distintos nodos. En las direcciones anycast, un paquete que es enviado a una dirección anycast, se entrega a la interface más cercana identificada por la dirección anycast.

Multicast: Es una dirección para un grupo de interfaces que por lo general pertenecen a distintos nodos. Un paquete que se envía a una dirección multicast se entrega a todos las interfaces identificadas por la dirección multicast.

1.5.2.3.2 Direcciones. Multicast.

Multidifusión o multicast es el envío de la información en una red a múltiples destinos simultáneamente, (pero no a todos), usando la estrategia más eficiente para el envío de los mensajes sobre cada enlace de la red sólo una vez y creando copias cuando los enlaces en los destinos se dividen. En comparación con multicast, los envíos de un punto a otro en una red se le denomina unidifusión (unicast), y el envío a todos los nodos en una red se le denomina difusión amplia (broadcast). Una situación frecuente donde se utiliza multicast es en la distribución de audio y vídeo en tiempo real a un conjunto de ordenadores que se han unido a una conferencia distribuida (NA, 2007a).

Soto (2006), afirma que en redes TCP/IP, estos receptores son representados por una dirección de grupo o dirección *multicast*. Esta dirección de grupo corresponde a una dirección IP que pertenece, en redes con el actual protocolo IPv4, a la antigua clase D, es decir, en la franja entre 224.0.0.0 y 239.255.255.255.

Una dirección multicast en IPv6, puede definirse como un identificador para un grupo de nodos. Un nodo puede pertenecer a uno o varios grupos *multicast*.

El “Identificador de Grupo”, identifica, como cabe esperar, el grupo de multicast concreto al que se refiere, bien sea permanente o temporal, dentro de un determinado ámbito. Por ejemplo, se asigna una dirección multicast permanente, con el identificador de grupo 101 (hexadecimal), al grupo de los servidores de tiempo (NTS), entonces:

FF01::101 significa todos los NTS en el mismo nodo que el paquete origen FF02::101 significa todos los NTS en el mismo enlace que el paquete origen FF05::101 significa todos los NTS en el mismo sitio que el paquete origen FF0E::101 significa todos los NTS en Internet .

Las direcciones multicast no-permanentes, sólo tienen sentido en su propio ámbito. Por ejemplo, un grupo identificado por la dirección temporal *multicast* local de sitio FF15::101, no tiene ninguna relación con un grupo usando la misma dirección en otro sitio, ni con otro grupo temporal que use el mismo identificador de grupo (en otro ámbito), ni con un grupo permanente con el mismo identificador de grupo.

Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6**,** ni aparecer en ninguna cabecera de encaminado. Las principales *direcciones multicast* reservadas son las incluidas en el rango FF0x:0:0:0:0:0:0:0.

Algunos ejemplos útiles de direcciones multicast**,** según su ámbito, serían:

FF01:0:0:0:0:0:0:1 – todos los nodos (ámbito local).
FF02:0:0:0:0:0:0:1 – todos los nodos (ámbito de enlace).
FF01:0:0:0:0:0:0:2 – todos los routers (ámbito local).
FF02:0:0:0:0:0:0:2 – todos los routers (ámbito de enlace).
FF05:0:0:0:0:0:0:2 – todos los routers (ámbito de sitio).

La dirección FF02:0:0:0:0:1:FFxx:xxxx, denominada “Solicited-Node Address”, o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la *unicast o anycast* de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso (“x”) por los mismos bits de la dirección original.

Así, la dirección 4037::01:800:200E:8C6C se convertiría en FF02::1:FF0E:8C6C. Cada nodo debe de calcular y unirse a todas las *direcciones multicast* que le corresponden para cada *dirección unicast y anycast* que tiene asignada.

El *multicast* está orientado hacia aplicaciones del tipo "uno a muchos" y "muchos a muchos". En estos casos, presenta claras ventajas cuando se le compara con los mecanismos de transmisión *unicast* y *broadcast*. Entre las diversas aplicaciones que pueden obtener ganancias con el uso de multicast están: videoconferencias; aprendizaje a distancia; distribución de software, noticias e informaciones de mercado; conciertos “en vivo”; actualización de bases de datos; juegos distribuidos; procesamiento competidor; simulacros distribuidos etc (Castorina, 2004).

1.5.2.3.3 Protocolos de enrutamientos multicast utilizados en IPv6.

Para poder informar a otros enrutadores sobre fuentes y destinos de multicast se deben emplear protocolos de enrutamiento. Castañeda y Colaboradores (2007), plantean que existen tres categorías básicas:

- Protocolos de Modo Denso (DVMRP y PIM-DM)
- Protocolos de Modo Sparse (PIM-SM y CBT)
- Protocolos de Estado de Enlace (MOSPF)

Estos autores alegan que los protocolos del tipo “Dense” (DM) utilizan el árbol más corto junto con un mecanismo de empuje, el cual asume que en cada interfaz del enrutador existe al menos un receptor del grupo. El tráfico es enviado (flooded) a través de todas las interfaces. Para evitar el desperdicio de recursos, si un enrutador no desea recibir tráfico envía un mensaje de supresión (prune). Como resultado se tiene que el tráfico de multicast sólo es enviado a los enrutadores que tienen miembros de grupos multicast. Este comportamiento de “Flood” y “Prune” se repite aproximadamente cada 2 o 3 minutos dependiendo del protocolo, por esta razón protocolos del tipo denso son mayormente empleados en ambientes LAN y donde el número de receptores usualmente es alto comparado con el de las fuentes y donde el ancho de banda no es un factor restrictivo. Protocolos basados en modo denso son el Distance Vector Routing Protocol (DVMRP) y el Protocol Independent Multicast Dense Mode (PIM-DM).

Los protocolos del tipo “Sparse” (SM) hacen uso del modelo de árboles compartidos y ocasionalmente como el PIM Sparse Mode (PIM-SM) del camino mas corto del arbol (Short Path Tree, SPT) para la distribución de tráfico multicast. Utilizan un mecanismo contrario al de los protocolos de modo denso, que asume que no existen receptores interesados en el tráfico de multicast, de esta forma ningún tráfico es enviado a menos que exista una solicitud explícita. Para que el árbol compartido sea construido, el enrutador receptor debe enviar a la raíz una solicitud de unión al árbol (Join message). Este mensaje viaja de enrutador a enrutador construyendo a su paso el camino hacia la raíz. Cuando un receptor desea dejar de recibir tráfico, debe enviar un mensaje de supresión (Prune) al igual que lo hacen los DM. Por su mecanismo contrario al de empuje, los protocolos SM son utilizados en ambientes WAN donde el ancho de banda es escaso o cuando se tienen más fuentes que destinos.

El punto más crítico de estos protocolos es el “Rendezvous Point” (RP) ya que si este no está bien ubicado por el administrador de la red puede ocasionar que el camino fuente-destino no sea el óptimo o que por exceso de tráfico el RP se convierta en un cuello de

botella. PIM-SM cuenta con un mecanismo que permite conmutar de árbol compartido a SPT para una fuente en particular.

Los protocolos de estado de enlace como Multicast Open Short Path First (MOSPF) hacen uso del “Short Path First” (SPF). Para construir estos árboles, los enrutadores envían información de estados de enlace que identifica la ubicación en la red de los grupos de miembros de multicast. Con esta información los enrutadores forman un SPT de cada fuente hacia todos los receptores en el grupo. Entre estos, podrían citarse el Distance Vector Multicast Routing Protocol (DVMRP), el multicast Open Shor Path First (MOSPF), Protocol Independent Multicast Dense Mode (PIM DM), el Protocol Independent Multicast Sparse Mode (PIM SM), Multicast Border Gateway Protocol (MBGP) y Multicast Source Discovery Protocol (MSDP).

Para la *arquitectura de IP multicast dentro del mismo dominio* (inter-dominio), se sugiere el uso de PIM Sparse Mode. Con PIM SM se eliminará el innecesario tráfico de multicast por los enlaces WAN. Se recomienda además que los RP sean descubiertos de forma automática por los enrutadores de tal forma que el proceso sea más eficiente y a prueba de fallas. El protocolo que se recomienda es el Bootstrap Router RFC 2362 (PIMv2). Aunque este protocolo es un poco más complejo que el Auto-RP (propietario de Cisco) asegura la interoperabilidad con enrutadores de otras marcas. Esto además de evitar la configuración estática de los RPs, asegura una redundancia en caso de falla de los RPs.

Finalmente se recomienda que las interfaces se configuren como de tipo sparse-dense, de tal forma que si todos los RP fallan, la red tenga oportunidad de conmutar a modo denso evitando que se pierda tráfico (Castañeda et al., 2007).

1.5.2.3.4 Asignación de direcciones.

Existen dos tipos de asignación de direcciones IP: con estado y sin estado. La asignación sin estado usa un proceso llamado Router Advertisement (RADV) y permite a los clientes obtener una IP y una ruta predeterminada simplemente levantando el dispositivo de una red. Se denomina 'sin estado' porque no se guarda ningún registro del estado de las IPs asignadas y las máquinas a las cuales se les ha asignado. La asignación 'con estado' se maneja mediante DHCPv6. Se llama así porque el servidor mantiene un registro con el estado de los clientes que han solicitado una IP y la han obtenido (Johanson, 2006).

La asignación sin estado usa un proceso llamado Router Advertisement y permite a los clientes obtener una IP y una ruta predeterminada simplemente levantando el dispositivo de una red, la determinación de los DNS se hace de manera automática.

Según Sedano (2001), el DHCPv6 (Dynamic Host Configuration Protocol Versión 6), utiliza direcciones multicast para enviar la mayoría de sus mensajes. Inicialmente, el cliente debe detectar la presencia de routers en el enlace utilizando mensajes de descubrimiento de vecino. Si un router es encontrado el cliente examina los mensajes enviados por el router para determinar si hay la necesidad de utilizar DHCP. Si los mensajes del router habilitan el uso de DHCP en el enlace o si no se encuentra ningún router, el cliente empieza una fase de solicitación DHCP con el fin de encontrar un servidor de DHCP.

Palet (2006), llama a la configuración *sin estado*, stateless, y la describe planteando que no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de routers y no precisa servidores adicionales. Permite generar a un host su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers: éstos anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras que el host genera un "identificador de interfaz", que identifica de manera única la interfase en la subred. La dirección se compone de la combinación de ambos campos. En ausencia del router, una estación de trabajo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace

En la configuración *con estado*, llamada también por Palet (2006), statefull, se obtienen tanto la dirección IP de la interfase, como la información y parámetros de configuración desde un servidor DHCP.

1.5.2.4 Seguridad.

Villa (2004), es del criterio que la implementacion de la seguridad a nivel de red, en el caso del protocolo IPv6, protege los niveles superiores y es transparente a las aplicaciones, las cabeceras de autenticación posibilitan autenticación y confiabilidad del origen de los datos. No incluye integridad de los datos pues el datagrama IPv6 no es encriptado, todo esto ayudara a eliminar algunos ataques comunes como IP spoofing y host masquerade.

Las cabeceras de encriptación RFC 2406 (Kent y Atkinson 1998), indican que estas brindan integridad y confidencialidad a los datagramas IPv6 ya que utiliza el algoritmo DES, encripta el encabezado de nivel de transporte y los datos, puede encriptarse el datagrama IPv6 completo de ser necesario.

1.5.3 Estado actual del protocolo IPv6 con relación a su utilización a nivel mundial y en Cuba.

Las redes académicas ya han comenzado la introducción acelerada de IPv6 en sus infraestructuras. Varios países, tales como Japón, Corea, China, EEUU y otros donde existe escasez de direcciones IPv4, han comenzado la transición y disponen ya de diversos servicios comerciales (Atkinson, 1998).

La industria de la telefonía móvil es un soporte muy fuerte para la transición a IPv6 en correspondencia el instituto europeo de estándares de las telecomunicaciones (ETSI) y el foro IPv6 ha establecido un acuerdo de cooperación para aunar sus fuerzas para lograr un mejor servicio al cliente (Hernández, 2006).

En Norteamérica muchas actividades relacionadas con IPv6, tanto en términos de estandarización y verificación, tienen sus orígenes en esta región. Muchas de estas actividades pueden ser localizadas en torno al “6bone”, la plataforma de pruebas internacional de IPv6. A corto plazo, seran palpables muchos ejemplos de nuevas actuaciones en México, Corea, India, Australia y Singapur ya que son países con alto nivel tecnológico. Hay una gran especulación acerca de que esto se convertirá en una gran fuerza según aumente el número de dispositivos de usuario final, como teléfonos móviles y adaptadores de televisión por cable, que requieren direccionamiento IP, lo que obligará a los desarrolladores a escoger IPv6 frente a IPv4 para permitir direcciones únicas para cada dispositivo (Palet, 2003).

Alfonso (2006), afirma que en Cuba ya existen redes IPv6 en los equipos troncales de la red y en todos los servidores, LACNIC ya asignó un bloque de direcciones IPv6 que fue aprobado y se encuentra en proceso legal de contratación, puede darse un servicio de registro de records IPv6 en el DNS.cu. para probar aplicaciones ya existentes en IPv4 sobre IPv6.

Sin embargo, se pudo comprobar en esta investigación, que efectivamente, Cuba se encuentra ya conectada al back bone IPv6, pero no existen redes con este protocolo que estén enlazadas a redes globales, incluso, se comprobó que existió un intento de crear una red nacional IPv6 en RedUniv, y no fue posible, pués los routers pertenecientes al suministrador de servicios, ETECSA, por los que debe fluir la comunicación entre los nodos de RedUniv, no soportan el IPv6, o no permiten este tipo de tráfico.

González (2005), menciona que existe un grupo que trabaja en la asimilación e investigación del Protocolo IPv6, el Grupo IPv6 Cuba ha generado y publicado el Portal IPv6 www.cu.ipv6tf.org con reconocimiento nacional e internacional. Desde el mes de abril del 2005 a la fecha, instituciones educacionales cubanas del MES, han obtenido bloques

de direcciones IPv6 dadas por RedUniv. El Ministerio de Educación Superior (MES), ha presentado a discusión su propuesta de implementar su Red en base al protocolo IPv6. Se trabaja de manera acelerada en una Política Nacional para la introducción del IPv6 en todo el país.

Los aspectos mas relevantes es que CITMATEL ya tiene configurado y operativo el servicio de DNS primario para el dominio .cu. El ISP de ETECSA también tiene operativo IPv6 su servidor DNS. Se trabajó en una configuración de conectividad internacional con el proveedor SEABONE por parte del NAP. Se trabajó por parte de los ISP en la configuración de la conectividad ISP – NAP. En el mes de noviembre de 2005 se levanto con NewCom (Proveedor de Internet de ETECSA) en Estado Unidos una conexión nativa IPv6 (Alfonso, 2006).

El mencionado autor indica que el nuevo protocolo de Internet, IP versión 6 (IPv6), ha venido a dar respuesta tecnológica al desarrollo de nuevos servicios y aplicaciones basados todos en infraestructura IP y a la necesidad creciente de garantizar la calidad de servicio en las presentes y futuras redes que emplean la tecnología Internet. Cuba no se encuentra ajena a estos cambios tecnológicos y más cuando se define como línea estratégica para el desarrollo socio-economico, al servir de soporte a otros sectores de la economía y de la sociedad.

1.5.4 Forma de solucionar las limitaciones del IPv4, ventajas de la utilización del IPv6.

Escasez de direcciones IP trae consigo menos direcciones disponibles, limita el crecimiento de Internet, obstaculiza el uso de Internet a nuevos usuarios, hoy día el ruteo es ineficiente y provoca que los usuarios usen NAT. Una de las limitaciones del IPv4 es que no fue diseñado para ser seguro. La forma de solucionar las limitaciones de IPv4 es implementar el IPv6 ya que con las nuevas tecnologías dicho protocolo esta quedando obsoleto (Kent y Atkinson, 1998) .

Las ventajas principales de la utilización del IPv6, consisten en que aumenta el rango de direcciones IP, simplifica el formato de la cabecera, mejor soporte para extensiones y opciones, se introducen etiquetas para distinguir flujos, se introducen opciones para seguridad y privacidad (Gonzalez, 2005).

1.5.4.1 Estudio comparativo entre el IPv4 e IPv6.

El desarrollo del Protocolo de Internet versión 6 (IPv6) no se trata de un cambio radical de protocolo, sino que es una evolución del anterior protocolo IPv4. Esto quiere decir que

aquellas características que son útiles y muy usadas en IPv4 se mantuvieron y otras se mejoraron, de tal manera que IPv6 presentará similares características y ventajas sobre IPv4 (Hernández, 2006).

1.5.4.2 Mayor espacio de direccionamiento.

La disponibilidad de prácticamente un número ilimitado de direcciones IP es el beneficio más evidente de la implementación de redes con IPv6. En comparación con IPv4, IPv6 incrementa el número de bits para direcciones en un factor de 4, de 32 bits a 128 bits. Los 128 bits proveen aproximadamente $3{,}4 \times 10^{38}$ direcciones, que son suficientes para que cada persona en el planeta posea 1030 direcciones (Gai, 1998).

La posibilidad de proveer de una dirección única para cada dispositivo de red permite facilidad de comunicación punto a punto, lo que es especialmente importante para la telefonía IP residencial. Además, IPv6 provee soporte completo para protocolos de capa aplicación sin requerir ningún tipo de procesamiento especial en los bordes de la red, eliminando los problemas asociados con NAT (Deering, 1998).

1.5.4.3 Cabeceras simplificadas.

A pesar de que el aumento en el número de bits en la dirección de IPv6 significa que se incrementa el tamaño de la cabecera, el formato de la cabecera IPv6 es más simple en comparación con la de IPv4 como lo observamos en la figura 1.12. El tamaño de la cabecera IPv4 básica es solo de 20 octetos, pero la longitud variable del campo de opciones la puede hacer mucho más grande. La cabecera IPv6 tiene un tamaño definido de 40 octetos. En la cabecera de IPv6, 6 de los 12 campos de la cabecera IPv4 fueron removidos, otros se mantuvieron con nombres modificados y otros campos han sido añadidos para mejorar la eficiencia e introducir nuevas características (Hagen, 2002).

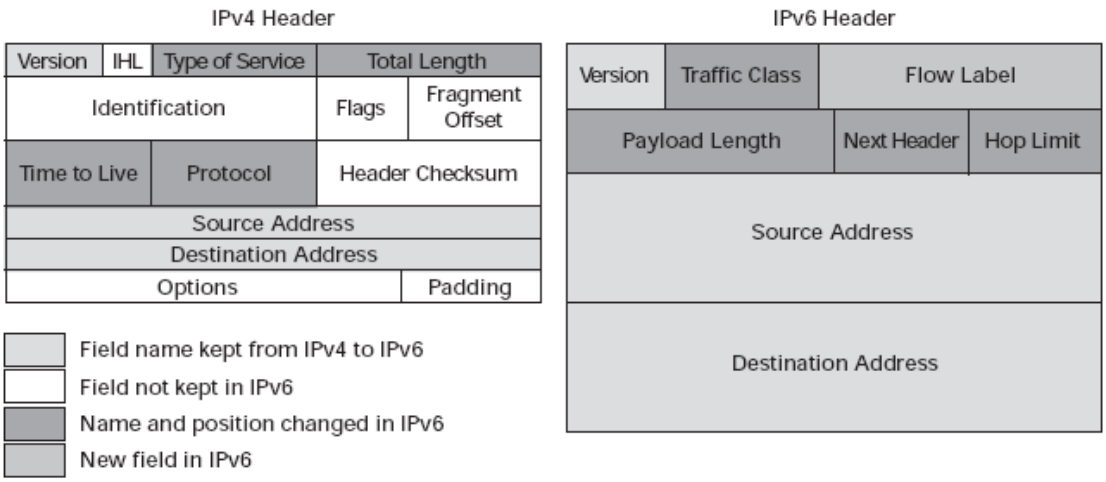

Figura 1.12 Comparación de las cabeceras IPv6 e IPv4

La fragmentación en IPv6 según Gai (1998), se maneja de diferente manera y no requiere de los campos presentes en la cabecera IP básica. Los routers ya no hacen fragmentación en IPv6, lo que evita problemas de procesamiento que se encontraban en los routers que manejaban fragmentación en IPv4. También, la remoción del campo Checksum permite una mayor eficiencia de los ruteadores.

1.5.4.4 Arquitectura de red.

La disponibilidad de un gran espacio de direccionamiento provee una arquitectura de red flexible. Esta flexibilidad permite que una organización utilice un solo prefijo de red para toda la red de la organización (Hagen, 2002).

El anterior autor menciona que un mayor espacio de direcciones permite también bloques más grandes de direcciones para los ISPs. Esto permitirá que los ISPs logren la sumarización de todos sus clientes en un solo prefijo, anunciando solo este prefijo en el Internet.

La jerarquización de las direcciones IP es otra de las ventajas de tener un mayor espacio de direccionamiento. En cada nivel se logrará la sumarización del tráfico solo a ese nivel, mejorando la asignación de direcciones de manera jerárquica.

Finalmente, Gonzalez (2005), refuta que esta jerarquización reduce el tamaño de las tablas de ruteo. Sin esquemas de direccionamiento jerárquicos, los ruteadores tendrían que almacenar tablas de ruteo muy grandes. En IPv4 este problema se resuelve parcialmente con CIDR (classless interdomain routing) y VLSM (variable length subset masking), pero estos métodos no son escalables ni eficientes.

1.5.4.5 Autoconfiguración y soporte plug and play.

La característica de auto-configuración de direcciones está incluida en el protocolo IPv6, permitiendo a un gran número de hosts fácilmente descubrir la red y obtener una dirección IPv6 nueva y globalmente única asociada con su locación. La auto-configuración permite el despliegue de dispositivos “plug-and-play”, como celulares, dispositivos inalámbricos, entre otros. De esta manera, los dispositivos de red podrían ser conectados sin la necesidad de una configuración manual ni de servidores, tales como un servidor DHCP (Hagen, 2002).

Kent y Atkinson (1998), mencionan que la auto-configuración, además, hace que una red existente se pueda renumerar simple y fácilmente. Mediante los mensajes de publicación y solicitación, explicados anteriormente, los hosts aprenden automáticamente el nuevo prefijo de red y lo usan para crear sus nuevas direcciones IP.

1.5.4.6 Eliminación de la necesidad de utilizar NAT.

Con la disponibilidad de un gran número de direcciones IPv6 para proveer direcciones globalmente únicas para todos los dispositivos IP, no existe necesidad de traducir cientos de direcciones IP internas a pocas direcciones IP globales. Al eliminar la necesidad de implementar NAT en las redes también se están eliminando otros problemas asociados con éste. Particularmente, la eliminación de NAT provee transparencia punto a punto, reduce la complejidad de la red y ayuda a reducir costos operacionales para los ISPs especialmente (Hagen, 2002).

1.5.4.7 Seguridad con implementación de IP Security.

Mientras que el uso de IPSec es opcional en IPv4, en IPv6 es obligatorio y es parte del protocolo. Por lo tanto, se puede habilitar IPSec en cada nodo IPv6, haciendo que las redes sean más seguras (Villa, 2004).

Gai (1998), opina que IPv6 provee cabeceras de extensión de seguridad, logrando que la implementación de encriptación, autentificación y VPNs sea fácil. De esta manera IPv6 provee de servicios de seguridad como control de acceso, confidencialidad e integridad de datos sin la necesidad de Firewalls adicionales que pueden introducir problemas, como cuellos de botella.

1.5.4.8 Mayor número de direcciones multicast.

Una de las más ventajosas características de IPv6 es que no usa broadcasts. Las funciones que utilizaban broadcasts en IPv4, como descubrimientos de routers, utilizan ahora multicast, además que el multicast es nativo en IPv6. Multicast permite que ciertos paquetes IP, como flujos de video, puedan ser enviados a múltiples destinos al mismo tiempo, ahorrando ancho de banda. Esta característica mejora la eficiencia de la red, limitando los requerimientos de broadcast a un número pequeño de nodos interesados. Además, IPv6 usa grupos específicos de direcciones multicast para diferentes funciones. En definitiva, el uso de multicast en IPv6 previene los problemas causados por tormentas de broadcast en las redes IPv4 (Gai, 1998).

1.5.4.9 Calidad del Servicio (QoS).

Cambronero (2001), alega que QoS en IPv6 se maneja de la misma manera de como se maneja en IPv4. Además, IPv6 soporta clase de servicio (CoS) mediante el campo clase de tráfico presente en la cabecera para poder dar servicio diferenciado. También, la cabecera IPv6 posee un campo llamado Etiqueta de flujo, donde se puede etiquetar flujos específicos, como video o video-conferencia. Cuando un flujo se encuentra etiquetado los

dispositivos presentes a lo largo de su camino tomarán acciones apropiadas basadas en la etiqueta.

1.6 Conclusiones del capítulo.

Hoy por hoy, IPv6 es la única manera de garantizar el crecimiento sostenido de Internet en los próximos años. Actualmente las comunicaciones basadas en IP se han implantado con gran fuerza en el mundo de las Telecomunicaciones, hasta tal punto que la arquitectura de red más grande del planeta y que comunica a más de 350 millones de personas tiene sus bases sobre el protocolo de red IP.

Durante años el protocolo IP ha logrado escalar redes de datos de manera eficiente y, en la actualidad, gracias a diversas herramientas como NAT, y el uso de proxys, lo sigue haciendo.

Los recursos originales considerados durante el diseño del protocolo IP se están agotando a una velocidad vertiginosa, de hecho, se calcula que para el 2012 se hayan agotado completamente las direcciones IP. Las direcciones de red disponibles para la conexión de los usuarios a la red pública (Internet) cada vez son más escasas, lo que ha hecho que el conseguir direcciones de red públicas sea cada vez más difícil y costoso. Además, en el diseño original del protocolo IP no se consideraron factores de seguridad y calidad de servicio, por lo que se han ido adecuando según las necesidades.

En IPv6 no solo existe una mayor capacidad de direccionamiento, sino que se incluyen características de seguridad y calidad de servicio, además de otros factores útiles para las redes de datos como una cabecera simplificada, auto-configuración, propiedades jerárquicas en el direccionamiento, facilidad de configuración para dispositivos móviles, entre otros.

Es inevitable que las redes de datos migren hacia el nuevo protocolo IPv6, no solo porque, eventualmente, el protocolo de red IPv4 agotará sus recursos de direccionamiento, sino porque IPv6 ha sido diseñado para que sea compatible con IPv4 y mejora las deficiencias que éste tiene.

Además con el surgimiento de millones de nuevos equipos con conectividad IP, las necesidades de incremento de direcciones y redes “plug & play” solamente se logran con la implementacion de IPv6.

El diseño de una red de datos debe proveer a la misma de funcionalidad, escalabilidad, adaptabilidad y administrabilidad. Estos 4 criterios son fundamentales para que una red de datos trabaje de forma óptima y pueda ir escalando tanto en tamaño como en tecnología.

2 Capítulo II. Instalación del protocolo IPv6 en la red de ordenadores de la Universidad de Granma.

2.1 Introducción.

En este capítulo se hace un análisis de las características de la red de la Universidad de Granma, exponiéndose la configuración IPv4 existente, lo que incluye segmentación de las redes, direcciones IP asignadas, sistemas operativos instalados, etc., también se da a conocer los principales servicios que ofrece la red UDG y las características de hardware de los servidores que en ella existen. Basándose en el análisis anterior se hace una valoración sobre la capacidad de soportar el protocolo IPv6 en los equipos y sistemas operativos existentes y se describen los pasos seguidos para superar las limitaciones tecnológicas existentes e instalar el protocolo IPv6.

2.2 Caracterización general de la Red Universitaria. Servicios que brinda.

La red de la Universidad de Granma, se basa actualmente en protocolo IP, versión 4.

La dirección de la red privada de la Universidad es la 10.24.0.0/255.254.0.0. La red pública es la 200.14.53.0/255.255.255.224.

La red UDG comprende las áreas:

1. Nodo Central ubicado en Bayamo, en la Calle Martí, número 68
2. Nodo Secundario de la Universidad de Granma, situado en el edificio del rectorado, segunda planta, área de Informática.
3. Nodo de la SUM de Río Cauto.
4. Nodo de la SUM de Cauto Cristo.
5. Nodo de la SUM de Jiguaní.
6. Nodo de la SUM de Bayamo.
7. Nodo del Laboratorio de Profesores, ubicado en Bayamo, calle Prolongación de General García, Nro 252.
8. Nodo de la SUM de Yara.
9. Nodo de la SUM de Manzanillo.
10. Nodo de la SUM de Campechuela.
11. Nodo de la SUM de Medialuna.
12. Nodo de la SUM de Niquero.
13. Nodo de la SUM de Pilón.
14. Nodo de la SUM de Bartolomé Masó.

15. Nodo de la SUM de Buey Arriba.
16. Nodo de la SUM de Guisa.

El nodo central, ubicado en Bayamo (Figura 2.1), posee varias redes o subredes: una destinada a servidores que se encuentran en una red interna con direcciones IP públicas (200.14.53.16/255.255.255.240) y otra a servidores que se hallan en una zona externa, o desmilitarizada (200.14.53.0/255.255.255.248). En la red interna se encuentran el servidor de correos (nostromo.udg.co.cu), el controlador de dominio primario y DNS interno (thot.udg.co.cu), el servidor de accesos remotos (200.14.53.30) y el servidor del Sistema Informatizado de Gestión de la Nueva Universidad (sigenu.udg.co.cu). En la red externa o desmilitarizada, se encuentra el servidor de correo entrante (mail.udg.co.cu) que es a su vez el www oficial de la Universidad, FTP y foros de discusión, el DNS externo (mediaserver.udg.co.cu) y MySQL, el proxy principal (proxy.udg.co.cu) y el servidor de mensajería instantánea (jabber.udg.co.cu). También existe una red de conexión con el router que hace el enlace con la red del campus universitario (192.168.250.0-255.255.255.248).

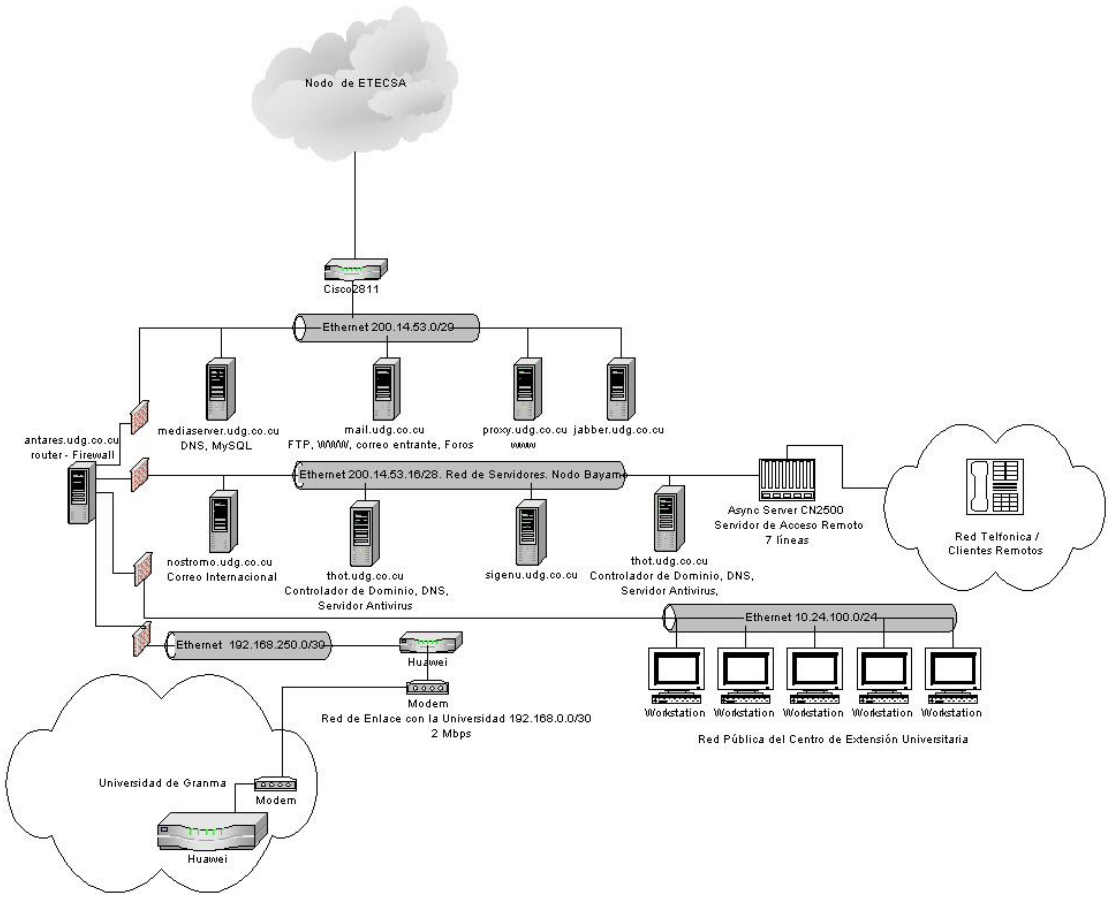

Figura 2.1 Esquema lógico de las redes del nodo central de Bayamo.

Existe además, una red pública en el edificio del Centro de Extensión Universitaria, en el que se encuentra instalado el nodo central, esta red, se conecta al resto a través del router antares.udg.co.cu, y su dirección es la 10.24.100.0/255.255.255.0.

La conexión a redes externas tales como Internet, RedUniv, u otras redes privadas cubanas (Infomed, Cubarte, etc), o a redes privadas (Sedes Universitarias Municipales, Laboratorios, etc); que se encuentran alejadas del campus universitario o del nodo central, se hace a través de un Router Cisco 2811 (Actualmente lo reemplaza un Cisco 4000 hasta que se arregle el 2811), que se halla en la red de la zona desmilitarizada del nodo de Bayamo, cuya IP, en la red 200.14.53.0/255.255.255.248 es la 200.14.53.1 (Figura 2.2).

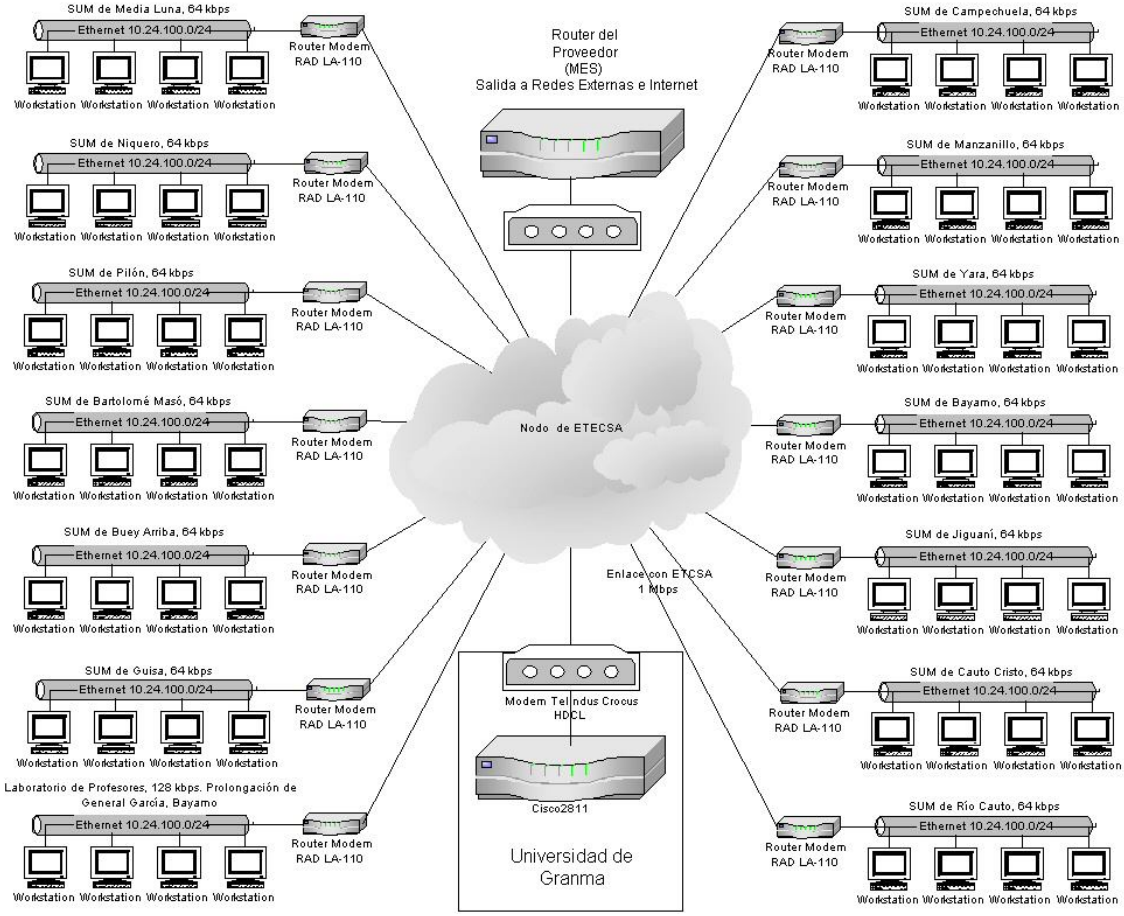

Figura 2.2 Enlaces del nodo central de Bayamo a las SUM y redes externas.

La Figura 2.2 refleja que este equipo posee una interfase Wan Física, y 15 virtuales: una para el enlace con el proveedor (MES), otra para el laboratorio de profesores de Bayamo

y el resto para las redes de las Sedes Universitarias Municipales, esto quiere decir, que para ello solo existe un canal arrendado a 2 mbps.

En la tabla siguiente (2.1), se relacionan los enlaces existentes entre el router principal de la red Universitaria, el proveedor y el resto de las instituciones pertenecientes a la Universidad, las cuales acceden a redes externas (Internet y RedUniv), y a las redes internas pertenecientes a la institución, a través de esta vía.

	Red de enlace	**Puerta de enlace predeterminada**	**Red interna**
Proveedor (RedUniv)	172.30.147.101/30	172.30.147.102	-
SUM Río Cauto	192.168.254.32/30	192.168.254.33	10.25.0.0/23
SUM Cauto Cristo	192.168.254.36/30	192.168.254.37	10.25.2.0/23
SUM Jiguaní	192.168.254.48/30	192.168.254.49	10.25.4.0/23
SUM Bayamo	192.168.254.4/30	192.168.254.5	10.25.6.0/23
SUM Yara	192.168.254.8/30	192.168.254.9	10.25.8.0/23
SUM Manzanillo	192.168.254.12/30	192.168.254.13	10.25.10.0/23
SUM Campechuela	192.168.254.16/30	192.168.254.17	10.25.12.0/23
SUM Media Luna	192.168.254.20/30	192.168.254.21	10.25.14.0/23
SUM Niquero	192.168.254.24/30	192.168.254.25	10.25.16.0/23
SUM Pilón	192.168.254.28/30	192.168.254.29	10.25.18.0/23
SUM Bartolomé Masó	192.168.254.44/30	192.168.254.45	10.25.20.0/23
SUM Buey Arriba	192.168.254.40/30	192.168.254.41	10.25.22.0/23
SUM Guisa	192.168.254.52/30	192.168.254.53	10.25.24.0/23
Laboratorio de Profesores de Bayamo	192.168.254.56/30	192.168.254.57	10.25.26.0/23

Tabla 2.1 Enlaces entre el Router principal de la Universidad de Granma, el proveedor y algunas dependencias.

Nótese que todo el conjunto de las redes de las Sedes Universitarias Municipales, se agrupan en el segmento de red 10.25.0.0/255.255.224.0. A todos los routers de las Sedes les será asignada la primera dirección IP disponible de cada LAN.

El enlace del nodo de Bayamo, con el nodo secundario ubicado en el campus universitario, se hace a través de un canal arrendado, a 2 mbps, con protocolo IP, para ello se utilizan 2 routers marca Huawei, modelo Quidway AR 28-09. La red de enlace entre los routers, es la 192.168.0.0/255.255.255.252, al enlace de Bayamo se le asignó la IP 192.168.0.1 y al extremo de la Universidad, la 192.168.0.2. (Figura 2.3).

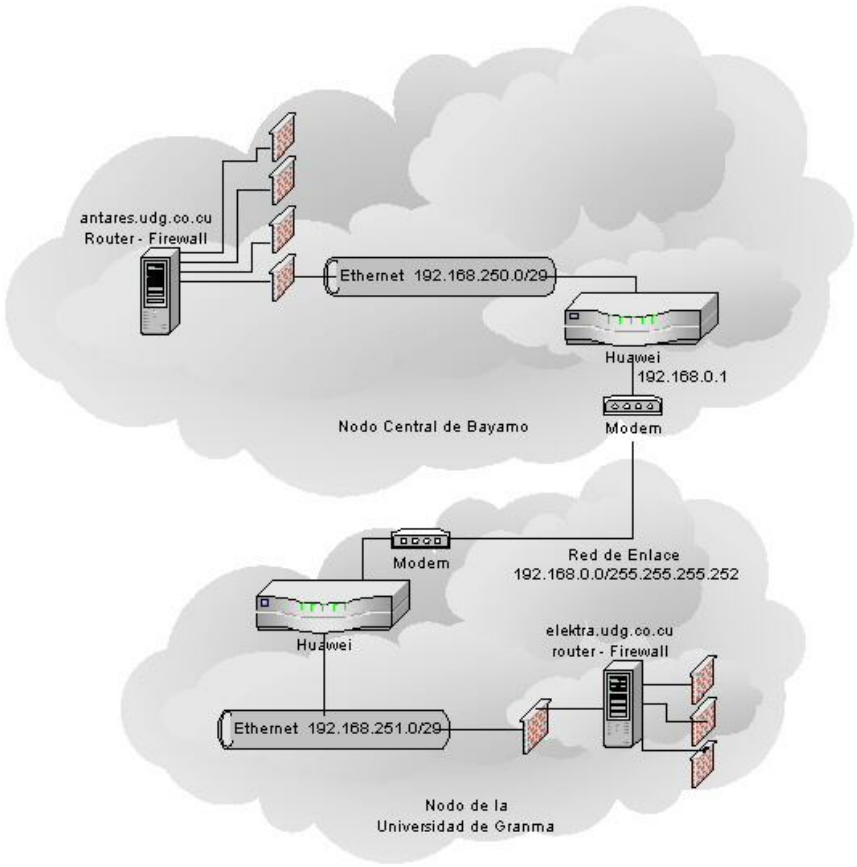

Figura 2.3 Enlace entre los nodos de Bayamo y Universidad

El router del nodo de Bayamo se conecta al servidor firewall y router antares.udg.co.cu, computadora con sistema operativo Linux Fedora Core 8, para ello, se designó la red 192.168.250.0/255.255.255.248, asignándosele al primero la IP 192.168.250.1 y 192.168.250.2 al segundo.

El router del nodo de la Universidad se conecta al servidor firewall y router elektra.udg.co.cu, computadora con sistema operativo similar al del nodo de Bayamo, para esto, se designó la red 192.168.251.0/255.255.255.248, asignándosele al primero, es decir, al router Huawei la IP 192.168.251.1 y al servidor Linux, que realiza las funciones de Router y firewall, la IP 192.168.250.2.

Caracterización de los equipos dedicados a servidores en el nodo central de Bayamo.

Los equipos utilizados como servidores en el nodo central están formados por computadoras IBM o PC compatibles, con procesadores del tipo Pentium IV, Pentium Dual Core y Xeon, siendo la mayoría los que poseen procesadores del tipo Pentium 4. El

sistema operativo mas utilizado es el Linux Fedora Core, versiones 6, 7 y 8, también existen servidores con Windows 2003 (Tabla 2.2).

Nombre del servidor	Interfaz de red	IP	Procesador	Memoria	Sistema Operativo	Servicios
antares.udg.co.cu	4	200.14.53.17 200.14.53.3 10.24.100.1 192.168.250.2	P4 2.8 GHz	256	Linux Fedora Core 8	Enrutamientos, Firewall.
thot.udg.co.cu	1	200.14.53.19	Dual Pentium 3 800 MHz	256	Windows 2003	Controlador de Dominio, Primario, DNS interno.
nostromo.udg.co.cu	1	200.14.53.18	Pentium Dual Core 3 GHz	1 G	Windows 2003	Correo Internacional, Cliente de correo Web.
sigenu.udg.co.cu	1	200.14.53.21	Xeon	1 G	Windows 2003	Servidor del Sistema de Gestión Universitaria (SIGENU)
mail.udg.co.cu	1	200.14.53.2	Pentium 4 Hyper Threating 2.8 GHz	1 G	Windows 2003	Servidor de Correo entrante o mail relay, portal de la Universidad de Granma (WWW) FTP, Foros de discusión y gráficos del mrtg.
mediaserver.udg.co.cu	1	200.14.53.4	Pentium Dual Core 3 GHz	512 M	Linux Fedora 6	DNS externo, Servidor de Bases de datos, MySQL y www
Proxy.udg.co.cu	1	200.14.53.5	Pentium Dual Core 3 GHz	512 M	Linux Fedora 6	Proxy principal, www.
jabber.udg.co.cu	1	200.14.53.6	Pentium IV 2.6 G	256 M	Linux Fedora Core 7	Servidor de mensajería instantánea

Tabla 2.2 Descripción de los servidores ubicados en el nodo de Bayamo y servicios que brindan.

Descripción de la red del campus universitario.

En la red informática de la sede central de la Universidad de Granma, existe una red ethernet que conecta al router del nodo Universitario con el servidor firewall y router elektra.udg.co.cu, computador con sistema operativo Fedora Core 6, el cual posee 4 redes conectadas a él, la primera con dirección 192.168.251.0/255.255.255.248, que se utiliza para la conexión del router Huawei y el router - firewall elektra.udg.co.cu , la

segunda red (10.24.1.0/255.255.255.0), es en la que se encuentran los servidores mas importantes del nodo, tales como hércules.udg.co.cu (10.24.1.2), con sistema operativo Windows 2003, el cual es el controlador de dominio primario, catálogo global, DNS y WINS; el servidor osiris.udg.co.cu (10.24.1.5) con sistema operativo Windows 2003 y presta servicios de SQL Server, el servidor Proxy, proxy1.udg.co.cu (10.24.1.16) con Fedora Core 6, el servidor de correo de estudiantes email.udg.co.cu (10.24.1.11), con Windows 2003. En esta red también se encuentran los servidores de archivos, todos con sistema operativo Windows 2003, agronomia.udg.co.cu (IP 10.24.1.12), informática.udg.co.cu (IP 10.24.1.14) e ingenieria.udg.co.cu (IP 10.24.1.15).

La tercera es la red pública o corporativa con dirección de red 10.24.6.0/255.255.254.0, ésta posee los servidores intranet.udg.co.cu (10.24.6.2, Fedora Core 6 y presta servicios de www, en éste se encuentra la página principal de la Web de la Intranet de la institución, también es un FTP y DHCP), odiseo.udg.co.cu (10.24.6.19, sistema operativo Linux Gentoo sus principales funciones consisten en hospedar servicios Web de los usuarios de la facultad de informática, tanto profesores como estudiantes), phraates.udg.co.cu (10.24.6.8, Windows 2003, controlador de dominio primario, DNS y WINS para la red corporativa), coppermine.udg.co.cu (10.24.6.18, sistema operativo Linux Ubuntu y ofrece actividades prácticas para los estudiantes de la facultad de informática), en esta red también se localiza el servidor de la biblioteca (ICT, 10.24.6.16), en cual ofrece servicios de archivos, Web, TFP, catálogo electrónico y biblioteca digital computarizada.

La cuarta es la red ethernet con dirección 192.168.4.0/255.255.255.0 es la correspondiente al área de economía o contable de la Universidad (Figura 2.4).

Caracterización de los equipos dedicados a servidores en el nodo de la Universidad.

Los equipos utilizados como servidores en el nodo universitario, están formados por computadoras IBM o PC compatibles, con procesadores del tipo Pentium III, Pentium IV, Pentium Dual Core y Xeon, siendo la mayoría los que poseen procesadores del tipo Pentium 4. Posee sistemas operativos tales como: Ubuntu 6.0, Gentoo; pero los sistemas operativos más utilizados son el Linux Fedora Core, versiones 6, 7, 8 y Windows 2003 (Tabla 2.3).

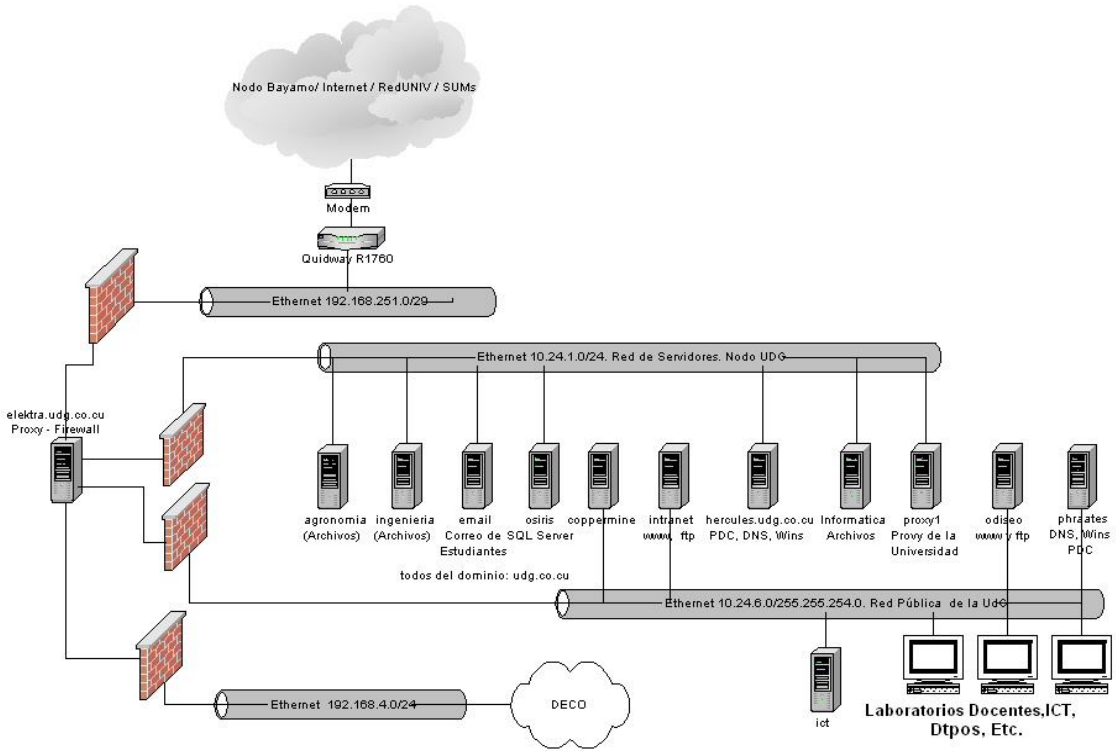

Figura 2.4 Esquema lógico del nodo de la Universidad de Granma.

Nombre del servidor	Interfaz de red	IP	Tipo de procesador	Memoria	Sistema Operativo	Servicios
elektra.udg.co.cu	4	192.168.251.2 10.24.1.1 10.24.6.1 192.168.4.1	Dual Pentium 3 800 MHz	256	Fedora Core 6	Firewall Enrutador
hercules.udg.co.cu	1	10.24.1.2	Intel Pentium IV 1.7 Ghz	512	Windows 2003	PDC(UDG) DNS, WINS
osiris.udg.co.cu	1	10.24.1.5	Intel Pentium III 934 Mhz	256	Windows 2003	SQL Server
phraates.udg.co.cu	1	10.24.6.8	Intel Pentium IV 1.7 Ghz	384	Windows 2003	Controlador de dominio Primario, DNS y WINS
intranet.udg.co.cu	1	10.24.6.2	Pentium Dual Core 3 GHz	512	Fedora Core 6	Web, TFP, DHCP
proxy1.udg.co.cu	1	10.24.1.16	Pentium Dual Core 3 GHz	512	Fedora Core 8	Proxy
odiseo.udg.co.cu	1	10.24.6.19	Intel Pentium IV 1.7 Ghz	512	Gentoo	Web hosting y FTP de la facultad de informática
coppermine.udg. co.cu	1	10.24.6.18	Intel Pentium III 934 Mhz	32	Ubuntu	Actividades practicas de los estudiantes de informática
email.udg.co.cu	1	10.24.1.11	Xeon	1 G	Windows 2003	Correo de los estudiantes
agronomia.udg.co.cu	1	10.24.1.12	Intel Celaron TM 1000 Mhz	128 Mb	Windows 2003	Web y Archivos
informatica.udg.co.cu	1	10.24.1.14	Intel Pentium IV 1.7 Ghz	640	Windows 2003	Archivos
ingenieria.udg.co.cu	1	10.24.1.15	Intel Pentium IV 1.7 Ghz	256	Windows 2003	Archivos
ict.udg.co.cu	1	10.24.6.16	Intel Pentium III 800 Mhz	256	Windows 2003	Archivos, Web, FTP, catalogo electrónico

Tabla 2.3 Descripción de los servidores ubicados en el nodo de la Universidad de Granma y servicios que brindan.

2.3 Análisis tecnológico del equipamiento actual y Limitaciones tecnologícas existentes para la instalación del nuevo protocolo.

Estaciones de trabajo de la red.

En investigaciones realizadas para la elaboración de este trabajo, se detectó que todos los ordenadores que forman la red universitaria son equipos de 32 bits, la inmensa mayoría con procesadores Pentium III y IV con 256 mega bytes de RAM, 5 computadoras Pentium II, y 4 ordenadores Pentium clásicos, con RAM entre 16 y 64 mega bytes. En las sedes universitarias municipales, todos los equipos tienen procesador Pentium IV, con 128 y 256 mega bytes de memoria interna u operativa.

Estos datos permitieron inferir que el 99% de las estaciones de trabajo de la red universitaria, por las características del hardware que poseen, soportan sistemas operativos, como Linux en diversas distribuciones, Windows 2000 o Windows XP aptos para el empleo del protocolo IPv6, pues solo existen 10 estaciones de trabajo con sistema operativo Windows 95. La red de cada Sede Universitaria Municipal tendrá próximamente capacidad para 24 computadoras y en la red de la Sede Central o Campus Universitario, la capcidad de estaciones de trabajo de la red ascendera a 1024.

Equipos de cómputo dedicados a servidores.

Servidores de propósito general o arquitectura IBM o PC compatible.

En las tablas 2.2 y 2.3 se han caracterizado anteriormente, las computadoras que se utilizan de manera dedicada a brindar servicios de red. Se destaca que el 52,38% del total (21), son máquinas expresamente dedicadas a este fin, sin embargo, todas poseen sistemas operativos que soportan el protocolo IPv6.

Servidores para propósitos específicos.

En este grupo se encuentran los routers o enrutadores utilizados en la institución, no obstante, es preciso aclarar que hay que excluir de aquí, los routers que se encuentran habilitados en computadoras de propósito general con arquitectura IBM o PC compatible, estos últimos son dos: el router - firewall de la Universidad de Granma, elektra.udg.co.cu, (ordenador marca Dell, modelo PowerEdge 1400, con 256 mega bytes de memoria y dos procesadores Pentium III a 800 MHz) y el router - firewall del nodo central de Bayamo (Hewlet Packard, modelo hp server tc2120, este equipo con una memoria de 256 mega bytes, y un procesador Pentium IV a 2.8 GHz); por lo tanto, en este acápite, se hará

referencia a los routers fabricados con este propósito solamente, los cuales son tres: el router principal de la institución: Cisco modelo 2811, los routers del enlace de la red del campus universitario con el nodo central, dos equipos marca Huawei, modelo Quidway AR 28 09.

El primero, es decir, el router Cisco, tiene instalada una versión del IOS (c2800nm-adventerprisek9-mz.123-8.T8) que soporta IPv6, sin embargo, la versión del IOS de los routers Huawei, no soporta este protocolo, y no fue posible obtener una que sí , a pesar de las gestiones hechas con el distribuidor local de estos equipos.

Los routers que se encuentran instalados en las Sedes Universitarias Municipales (SUM), son de dos clases: Modems – Routers, marca Telindus, modelo 1421 o 1423 y marca RAD modelo LA110, ninguno de los empleados soportan el protocolo que se pretende instalar, ni sus fabricantes brindan soporte para esto. El servidor de accesos remotos (Moxa CN2516) soporta el protocolo IPv6.

Otra limitación consiste en que el subministrador de servicio para el acceso a redes globales, no brinda la posibilidad de utilizar el protocolo IPv6 y esto no tiene una solución inmediata o a corto plazo por la infraestructura y las características de los routers y otros equipos existentes en la red nacional de transmisión de datos del suministrador.

2.3.1 Tipos de túneles, su utilización.

El túnel es un método por el cual se hace uso de una red intermedia para transferir datos de un extremo a otro. Los paquetes que se transmiten se encapsulan sobre otro encabezado correspondiente al protocolo de túnel, este nuevo encabezado contiene la información necesaria para que el paquete atravesando la red intermedia llegue al destino correspondiente, una vez llegados a destino son desencapsulados y dirigidos al destino final (Lockhart, 2007).

Sanlés y Vaamonde (2003), alegan que un túnel encapsula un protocolo de red dentro de los paquetes del mismo protocolo, que serán llevados por la red real. Adicionalmente, el paquete encapsulado es encriptado por el emisor, en acuerdo con el receptor (el sistema que se encuentra en el otro lado del túnel) de manera que sólo ambos extremos puedan acceder a los datos transportados. Éste tipo de comunicación solo es posible si el protocolo soporta esta facilidad, denominada *modo túnel*. La otra modalidad posible, *modo transporte*, provee protección sólo para protocolos de la capa superior.

La técnica de “tunneling” consiste en encapsular un mensaje de un protocolo dentro de sí mismo aprovechando ciertas propiedades del paquete externo con el objetivo de que el mensaje sea tratado de forma diferente a como habría sido tratado el mensaje

encapsulado. De esta forma un paquete puede saltar la topología de una red. Por ejemplo, un túnel puede ser usado para evitar un firewall (con los peligros consecuentes de esta decisión). Esta es una consideración a tener en cuenta al configurar un túnel (Van-Beijnum, 2005).

De esta forma, el túnel es simplemente la ruta que toman los paquetes encapsulados (y encriptados), dentro de un paquete del mismo protocolo, entre las dos redes. Un atacante puede interceptar los mensajes que viajen por el túnel, pero los datos encapsulados están encriptados y solo pueden ser recuperados por el destinatario final.

Sanlés y Vaamonde (2003), mencionan que la herramienta IP nos permite hacer tres tipos de túneles:

Túneles IPIP, donde se encapsula IPv4 sobre IPv4 para determinadas aplicaciones. Es decir el modo IPIP corresponde a un simple túnel IP sobre IP. Se encapsulan los paquetes sin más.

Túneles GRE (Generic Routing Encapsulation), donde se realiza un tráfico encriptado sobre IP. Los túneles GRE especificados por la compañía Cisco, son túneles IP sobre IP cifrados y permite establecer políticas de encaminamiento y seguridad.

Túneles SIT (Simple Internet Transition), donde se encapsula IPv6 sobre IPv4 de modo que podamos establecer una comunicación de un punto a otro punto con IPv4 pero que transportara IPv6. El modo SIT se usa para túneles IPv6.

En la implantación de IPv6 es habitual el uso de túneles, generalmente por motivos de compatibilidad, hay que tener en cuenta que IPv6 no está muy extendido y en muchos casos es habitual que haya que usar transporte IPv4 para llegar a zonas de uso IPv6, La mecánica es la habitual en todos los túneles, rellenar el campo de datos de un paquete IPv4 con paquetes IPv6 y una vez que hayan llegado al otro punto del transporte, se extraerán y dirigirán correctamente a las máquinas IPv6. En el caso de esta investigación, se utilizarán túneles del tipo SIT, para realizar comunicación IPv6 entre dos redes, teniendo como transporte IPv4. Este tipo de túnel fue creado específicamente con esta finalidad.

2.3.2 Soluciones técnicas a las limitaciones.

Es evidente, que no resulta posible dar solución absoluta a algunos de las dificultades detectadas durante la implementación de este novedoso protocolo en la red de la Universidad de Granma, por ejemplo, la falta de soporte, por parte del proveedor de servicios de comunicaciones para el acceso a redes basadas en IPv6, no obstante, se decidió continuar con esta investigación, pues, entre las directivas del Ministerio de

Educación Superior (MES), se encuentra la del establecimiento o instalación del protocolo IPv6 en todos los centros universitarios del país, de tal forma que, una vez que el suministrador se encuentre en condiciones de brindar soporte para ello, las universidades estén preparadas para el acceso a redes basadas en el protocolo que se está tratando (Internet II, CLARA, RedIris, Alfa, entre otras).

A pesar de lo antes mencionado, en las búsquedas e investigaciones realizadas, se detectó la existencia de servidores públicos y gratuitos para solucionar, al menos de manera parcial, esta limitante.

La mayor parte de los proveedores de Internet todavía no ofrecen conexiones IPv6 de modo nativo, en Cuba, ninguno. Para superar está barrera, existen en todo el mundo los llamados "tunnel brokers", que ofrecen gratuitamente la posibilidad de un enlace IPv4, a través de el cual, se encapsula el protocolo IPv6.

Como puede observarse en la siguiente tabla, los mismos se encuentran distribuidos prácticamente en todas las zonas geográficas del planeta, (tabla 2.4), existen muchos más, pero estos son los más destacados. La elección del tunnel broker a utilizar, se basó principalmente en la situación geográfica de los mismos, y las facilidades que estos pudieran brindar, por ende, el análisis para la elección se limitó a los Norteamericanos y Europeos.

A continuación, se hace una breve caracterización de los servidores “Túnel Brokers” que se valoraron para ser usados en esta experiencia.

Broker	Situación geográfica
Hurricane Electric	Estados Unidos y Canadá
Freenet6	Estados Unidos
SixXS	Europa
Singnet	Singapur
Aarnet	Australia, Pacífico Sur

Tabla 2.4 Servidores ¨Tunnel Brokers¨ mas destacados a nivel mundial.

Hurricane Electric (http://tunnelbroker.net). Hurricane Electric (HE) ofrece túneles IPv6 gratuitos y asigna un bloque de direcciones IPv6 para el cliente. También permite configurar un DNS inverso. Conseguir un túnel de HE es rápido, simple, seguro (https) y sencillo. Para ello es necesario registrarse, este paso incluye una lista de datos personales como la dirección y número de teléfono del cliente. Los túneles de HE tardan 24 horas en activarse, con el fin de evitar abusos.

Por otra parte, también resulta muy sencillo y fácil reconfigurar las propiedades del túnel. Algo importante es que los túneles de enlaces creados, éstos serán del tipo SIT. El extremo del cliente, puede hacerse utilizando plataformas Windows, Linux, Cisco y otros tipos de routers.

Cada vez que se crea un túnel, es asignada una red IPv6 de enlace para éste, y una red con prefijo 64 para asignar direcciones públicas IPv6 a las computadoras de la red privada, brindando la posibilidad de prescindir de este segmento y usar direcciones IPv6 ya asignadas por el NIC (BGP).

Se brindan ejemplos de configuración de varios sistemas utilizando varios sistemas operativos para la creación del túnel de enlace.

Muy rápida la entrada al sitio, dado principalmente por la sencillez de éste.

La configuración y creación del túnel es vía Web.

Freenet6 (http://www.freenet6.net). El proceso de registro es simple también, sin embargo, la creación de los túneles es un poco mas compleja, pues se basa en la obtención de un software que se encargará tanto de la creación como de la configuración del túnel de enlace, por ende, el mismo deberá descargarse e instalarse en la computadora que asumirá las funciones de router excluyendo la posibilidad de utilizar routers Cisco o de otra clase. Brinda una subnet con prefijo 64.

SixX (http://www.sixxs.net). Pertenece a Europa, y al igual que el anterior, la creación del túnel de enlace se basa en el uso de un software suministrado por el sitio. Hay que destacar que hay soporte multiplataforma (Linux, freeBSD y Windows) y la posibilidad de hacer NAT, ofrece un segmento con prefijo 48 para la subnet.

Por los elementos hasta aquí mencionados, se decidió probar la conexión a la red global y pública IPv6 utilizando el Tunnel Broker HE.

La existencia de este tipo de servicio constituyó un resultado no esperado en esta investigación, lo cual condicionó que se decidiera, no ofrecer aún acceso a la red pública IPv6 a los usuarios y estaciones de trabajo de la red corporativa, sino, limitarlo a modo experimental a la subnet de los servidores del nodo central de Bayamo; esta decisión se fundamentó en cuestiones que precisan solución previa a la utilización masiva de redes globales con IPv6, las cuales no constituyen objetivos de esta investigación, tales como elementos de seguridad informática, políticas actuales cubanas relacionadas con el acceso a la Internet con IPv6 que aún no están muy claramente definidas a nivel de país, la necesidad de evaluar el comportamiento de un proxy que soporte el protocolo estudiado, de manera que se pueda seguir el uso de la red en caso de necesidad y finalmente, la necesidad de probar la calidad de este tipo de servicio.

En la Figura 2.5, se destaca la manera en que se estableció el túnel SIT con el servidor de HE para el acceso a redes globales basadas en la versión 6 de IP.

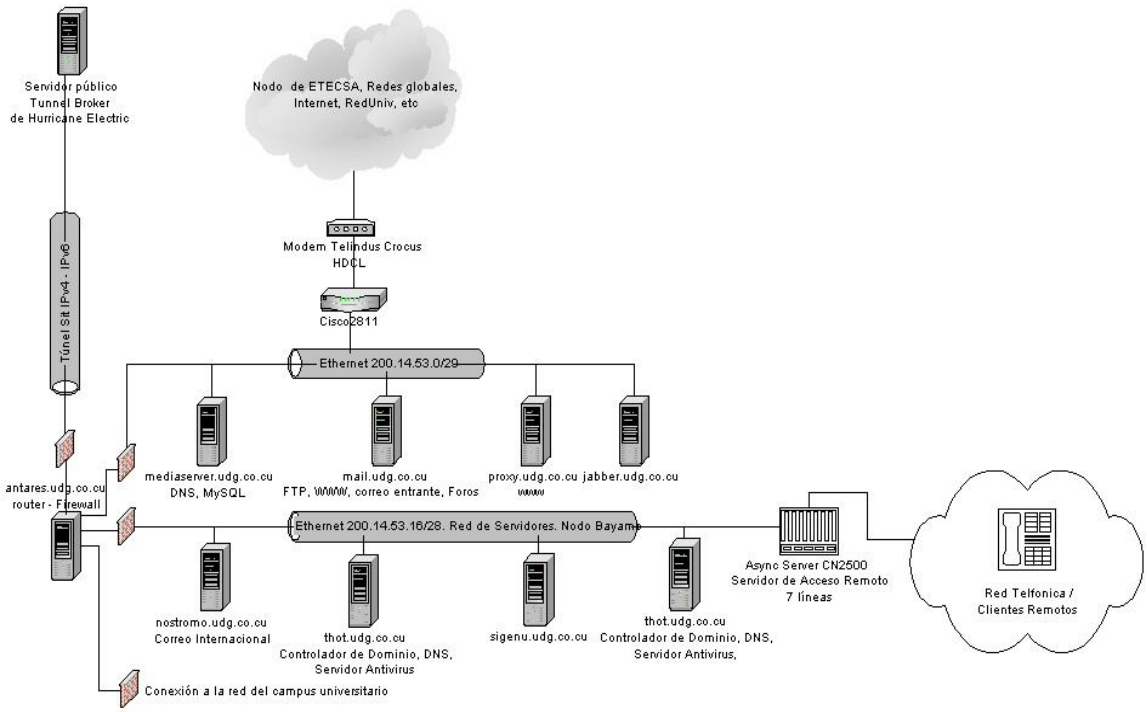

Figura 2.5 Conexión de la red de la Universidad de Granma con la red global IPv6.

Nótese que hubiera sido mucho más funcional colocar extremo local del túnel en el router principal (Cisco 2811), pero en estos momentos, el mismo está dañado y en espera de reparación y el que se encuentra reemplazándolo de manera provisional, un Cisco 4000, no soporta IPv6.

Otro problema de gran peso y que requería solución, era el de la falta de soporte para IPv6 por parte de los enrutadores que conectan las redes del campus universitario y la red de los servidores del nodo, para superar esta dificultad de manera inmediata (pues la solución definitiva sería la compra de routers que soportaran el protocolo IPv6), se implementó un túnel que fuese capaz de encapsular el protocolo IPv6 en datagramas IPv4, facilitado por las características topológicas de la redes que forman el enlace entre los nodos de Bayamo y Universidad, esto se puede comprender con mas facilidad si se analiza la anterior figura 2.3, en este caso, se notará que los routers Huawei, los cuales utilizan la red de enlace 129.168.0.0/255.255.255.252 para conectarse entre sí, no soportan el IPv6, pero, los routers - firewall, elektra.udg.co.cu y antares.udg.co.cu, sí; y éstos últimos se encuentran conectados directamente y mediante redes ethernet a los

huawei, por lo que resultó muy cómodo instalar un túnel que encapsulara el tráfico IPv6 en IPv4 entre las computadoras elektra.udg.co.cu y antares.udg.co.cu. (Figura 2.6)

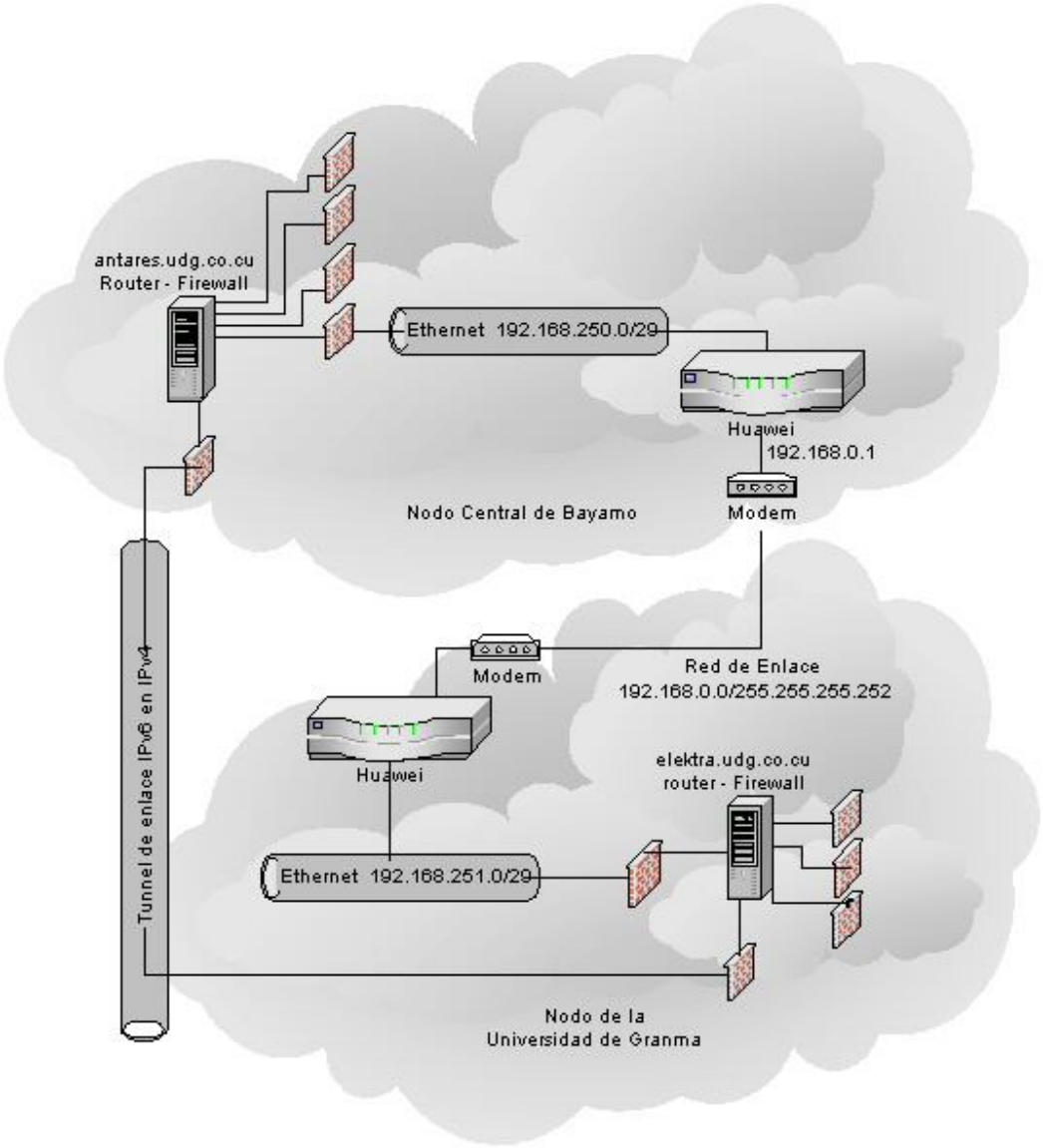

Figura 2.6 Túnel para el tráfico IPv6 entre los nodos Bayamo y Universidad.

Otro impedimento lo constituyó la instalación del IPv6 en las Sedes Universitarias Municipales (SUM), pues los routers con que éstas se enlazan al nodo principal no soportan el protocolo estudiado, esto se podría solucionar también mediante el uso de túneles, sin embargo, se detectó la existencia de un grupo de factores tales como la reducida cantidad de computadoras existentes en cada sede (8 estaciones de trabajo promedio), lo que dificulta que se asigne uno de los pocos ordenadores existentes para que se utilice como puerta de enlace predeterminada para el protocolo IPv6 en cada una

de las 13 sedes universitarias, no todas cuentan con un personal adecuadamente calificado para mantener trabajando una red con protocolo IPv6, y finalmente, las sedes se encuentran a gran distancia del nodo central, en algunos casos, éstas superan los 100 kilómetros, por lo que se requerirían recursos de transporte que no están comprendidos en el proyecto de este trabajo de diploma; que condicionaron la decisión de excluir, al menos en este trabajo investigativo, la instalación del protocolo IPv6 en las Sedes Universitarias Municipales de la Universidad de Granma.

2.4 Diseño del direccionamiento a partir del número de red asignado por el proveedor.

A pesar de que actualmente la Red Universitaria Cubana basa sus comunicaciones en el protocolo IPv4, la instalación del IPv6 constituye una política de gran peso en todos los organismos pertenecientes al Ministerio de Educación Superior (MES), con este fin, el proveedor de servicios de accesos a redes externas, perteneciente también al MES, distribuyó entre todas las instituciones de este ministerio, bloques de direcciones de redes IPv6 para condicionar la instalación de este protocolo a nivel nacional, sin embargo, hay que aclarar, que estas direcciones solo tienen un significado local en la red privada, pues no se corresponden con los segmentos asignados por LACNIC a Cuba, esto se debe a que el Ministerio rector encargado de esta actividad, aún no ha distribuido estos bloques de direcciones.

Las direcciones delegadas a Cuba según los registros estáticos regionales a Internet (RIR) son (Maigron, 2008):

2001:1340::/32

2001:1358:: /32

2001:1308:: /32

La dirección nacional de Informatización del MES, decidió, utilizar, para condicionar la creación de la red nacional con soporte a este protocolo, el bloque 2001:b00:f800::/44, y a la Universidad de Granma, le correspondió el segmento:

2001:b00:f80b::/52

2.4.1 Segmentación del bloque de IP (v6) asignado a la Universidad por el MES y asignación de direcciones IP fijas en las diferentes subredes.

El bloque de direcciones, asignado a la Universidad, se segmentó de la siguiente manera:

Primeramente, el bloque asignado se dividió en 16 subredes con prefijo 56:

2001:b00:f80b::/56
2001:b00:f80b:100::/56
2001:b00:f80b:200::/56
2001:b00:f80b:300::/56
2001:b00:f80b:400::/56
2001:b00:f80b:500::/56
2001:b00:f80b:600::/56
2001:b00:f80b:700::/56
2001:b00:f80b:800::/56
2001:b00:f80b:900::/56
2001:b00:f80b:a00::/56
2001:b00:f80b:b00::/56
2001:b00:f80b:c00::/56
2001:b00:f80b:d00::/56
2001:b00:f80b:e00::/56
2001:b00:f80b:f00::/56

El primer segmento (2001:0b00:f80b:0000::/56) se destinó al nodo central de Bayamo, lo que proporciona la posibilidad de dividirlo en 256 redes con prefijo /64: desde la 2001:0b00:f80b:0000::/64 hasta la 2001:0b00:f80b:00ff::/64.

A la red de la zona desmilitarizada del Nodo de Bayamo se le asignó el bloque (200.14.53.0/29 en IPv4):

2001:b00:f80b::/64

Asignaciones de direcciones IP específicas a los servidores que se encuentran en esta red:

2001:b00:f80b::1 – router
2001:b00:f80b::2 – mail.udg.co.cu
2001:b00:f80b::3 – firewall - router (antares.udg.co.cu)
2001:b00:f80b::4 – mediasertver (DNS)
2001:b00:f80b::5 – proxy.udg.co.cu
2001:b00:f80b::6 – jabber.udg.co.cu

A la red interna de los servidores (200.15.53.16/28) se le asignó el bloque IPv6 suministrado por el HE, puesto que esta red tendrá de momento acceso a sitios externos con este protocolo:

2001:470:1f07:239::/64

Asignaciones de direcciones IP específicas a los servidores que se encuentran en esta red:

2001:470:1f07:239::1 – router – firewall (antares.udg.co.cu)

2001:470:1f07:239::2 – nostromo.udg.co.cu
2001:470:1f07:239::3 – thot.udg.co.cu

A este segmento, se le reservó también otra dirección de red: la 2001:b00:f80b:1::/64, ésto, para el caso de que se deseche el segmento de red otorgado por HE, por ello, se reservaron a los servidores de esta red las direcciones IP:

2001:b00:f80b:1::1 – router – firewall (antares.udg.co.cu)
2001:b00:f80b:1::2 – nostromo.udg.co.cu
2001:b00:f80b:1::3 – thot.udg.co.cu

Las red 2001:b00:f80b:2::/64 se dejó de reserva para usos futuros.

A la red que se encuentra instalada en el Centro de Extensión Universitaria, edificación en la que se halla también el nodo central, se le asignó la dirección 2001:b00:f80b:4::/64, y dentro de ésta, se le colocó una dirección fija al router-firewall antares.udg.co.cu: 2001:b00:f80b:4::1/64.

El túnel se hizo entre las IP 192.168.250.2 (router firewall del nodo bayamo) y 192.168.251.2 (router firewall del nodo universidad), para ello, se empleó el bloque 2001:0b00:f80b:0003::/64, otorgándole la IP 2001:b00:f80b:3::1/64 al firewall de Bayamo y la 2001:b00:f80b:3::2 al firewall de la Universidad.

Quedan libre, a partir de la 2001:b00:f80b:4::/64 hasta la 2001:b00:f80b:ff::/64. También se deja de reserva, para posibles usos posteriores, el bloque 2001:b00:f80b:100::/56.

Al campus universitario o sede central, se le asignaron los bloques 2001:b00:f80b:200::/56 y 2001:b00:f80b:300::/56 el último como reserva para uso futuro.

El segmento (2001:b00:f80b:200::/56) proporciona la posibilidad de dividirlo en 256 redes con prefijo /64: desde la 2001:b00:f80b:200::/64 hasta la 2001:b00:f80b:2ff::/64.

El nodo Universitario recibió la dirección de red 2001:0b00:f80b:200::/64 (Red 10.24.1.0/24)

Asignaciones de direcciones IP específicas a los servidores que se encuentran en esta red:

2001:b00:f80b:200::1/64 – router – firewall (elektra.udg.co.cu)
2001:b00:f80b:200::2/64 – hercules.udg.co.cu
2001:b00:f80b:200::5/64 – osiris.udg.co.cu
2001:b00:f80b:200::b/64 – email.udg.co.cu
2001:b00:f80b:200::c/64 – agronomia.udg.co.cu
2001:b00:f80b:200::e/64 – informatica.udg.co.cu
2001:b00:f80b:200::f/64 – ingenieria.udg.co.cu
2001:b00:f80b:200::10/64 – proxy1.udg.co.cu

Quedan libres las redes 2001:b00:f80b:201::/64, 2001:b00:f80b:202::/64 y 2001:b00:f80b:203::/64.

La red del campus universitario, en la que se encuentran la totalidad de las estaciones de trabajo y usuarios (IPv4 10.24.6.0/23), recibió la dirección 2001:b00:f80b:204::/64, aquí se realizaron las siguientes asignaciones fijas:

2001:b00:f80b:204::1/64 – router – firewall (elektra.udg.co.cu)
2001:b00:f80b:204::2/64 – intranet.udg.co.cu
2001:b00:f80b:204::8/64 – phraates.udg.co.cu
2001:b00:f80b:204::10/64 – ict.udg.co.cu
2001:b00:f80b:204::12/64 – coppermine.udg.co.cu
2001:b00:f80b:204::13/64 – odiseo.udg.co.cu

Se dejarán de reserva, las redes 2001:b00:f80b:0205::/64, 2001:b00:f80b:206::/64 y 2001:b00:f80b:207::/64.

A la red del área económica, se le destinó la dirección 2001:b00:f80b:208::/64, en la que se asignaron las IP fijas a los servidores:

2001:b00:f80b:208::1 – router - firewall (elektra.udg.co.cu)
2001:b00:f80b:208::2 – servidor de contabilidad
2001:0b00:f80b:0400::/56 – Sedes Universitarias Municipales

A pesar de que en esta investigación no se implementó el protocolo IPv6 en las Sedes Universitarias Municipales, durante la segmentación del bloque de direcciones IP asignado, si se tuvieron en cuenta éstas, para un futuro. A las Sedes se les destinó el bloque 2001:b00:f80b:400::/56, lo que permite que cada SUM pueda disponer de un segmento con prefijo /62, posibilitando la existencia de 4 bloques con prefijo /64 en cada sede:

2001:b00:f80b:400::/62 – SUM Río Cauto
2001:b00:f80b:404::/62 – SUM Cauto Cristo
2001:b00:f80b:408::/62 – SUM Jiguaní
2001:b00:f80b:40c::/62 – SUM Bayamo
2001:b00:f80b:410::/62 – SUM Yara
2001:b00:f80b:414::/62 – SUM Manzanillo
2001:b00:f80b:418::/62 – SUM Campechuela
2001:b00:f80b:41c::/62 – SUM Media Luna
2001:b00:f80b:420::/62 – SUM Niquero
2001:b00:f80b:424::/62 – SUM Pilón
2001:b00:f80b:428::/62 – SUM Bartolomé Masó
2001:b00:f80b:42c::/62 – SUM Buey Arriba
2001:b00:f80b:430::/62 – SUM Guisa

El primer bloque con prefijo /64 de cada SUM, será utilizado para la red de enlace, el segundo se deja de reserva para usos futuros, el tercero será utilizado en la red

corporativa de cada sede, y el cuarto, de reserva, así, por ejemplo, para la SUM del Municipio de Río Cauto, la utilización de los bloques sería de la siguiente manera:

2001:b00:f80b:400::/64 – Red de enlace con la universidad
2001:b00:f80b:401::/64 – Reserva
2001:b00:f80b:402::/64 – Corporativa
2001:b00:f80b:403::/64 – Reserva

Quedan, para futuras implementaciones, a partir de la red 2001:b00:f80b:434::/62 hasta la 2001:b00:f80b:4fc::/62, estas pertenecientes, al bloque 2001:b00:f80b:400::/56, y los bloques o segmentos con prefijo /56:

2001:b00:f80b:500::/56
2001:b00:f80b:600::/56
2001:b00:f80b:700::/56
2001:b00:f80b:800::/56
2001:b00:f80b:900::/56
2001:b00:f80b:a00::/56
2001:b00:f80b:b00::/56
2001:b00:f80b:c00::/56
2001:b00:f80b:d00::/56
2001:b00:f80b:e00::/56
2001:b00:f80b:f00::/56

2.4.2 Planificación de las rutas IPv6.

2.4.2.1 Configuración de las rutas y las puertas de enlace en las redes del campus universitario.

En este tópico es necesario aclarar que todas las redes ubicadas en el campus se encuentran unidas entre sí por el mismo router: elektra.udg.co.cu (Figura 2.4), por ello, basta con que todos los integrantes de las diferentes redes, tengan, como puerta de enlace predeterminada (default gateway), la correspondiente a la dirección IP de la interfase de red del router que se encuentra en su propia red. Por lo tanto, la puerta de enlace predeterminada para todos los ordenadores que se ubican en la red de los servidores del nodo (2001:b00:f80b:200::/64), exceptuando el propio router, sería la dirección 2001:b00:f80b:200::1, la puerta de enlace predeterminada para la red pública o corporativa (2001:b00:f80b:204::/64) sería la IP 2001:b00:f80b:204::1, de igual manera, para todos los equipos pertenecientes a la red del área económica (2001:b00:f80b:208::/64), la puerta de enlace sería la IP del router para esa red: 2001:b00:f80b:208::1.

Al router – firewall le corresponde entonces, como puerta de enlace predeterminada, la dirección IP del router – firewall del nodo de Bayamo: 2001:b00:f80b:3::1, en la red de enlace, que es a su vez, el túnel.

En el anexo 1, se muestra la configuración de la red para el router elektra.udg.co.cu, esta información la contiene el archivo network, que se encuentra en el directorio /etc/sysconfig.

2.4.2.2 Diseño de las rutas y las puertas de enlace en las redes del Centro de Extensión Universitaria.

Actualmente la conexión a redes externas basadas en IPv6, se hace a través del router – firewall antares.udg.co.cu, por medio de un túnel de tipo SIT, por lo tanto, esta será la puerta de enlace predeterminada para todas las redes que a este router se conectan (Tabla 2.5).

Red		**Puerta de enlace**
Dirección de red	Función	
2001:b00:f80b::/64	Red de servidores de la zona desmilitarizada.	2001:b00:f80b::3
2001:470:1f07:239::/64 2001:b00:f80b:1::/64	Red interna de servidores.	2001:470:1f07:239::1 2001:b00:f80b:1::1
2001:b00:f80b:4::/64	Red del Centro de extensión Universitaria.	2001:b00:f80b:4::1
2001:470:1f06:239::/64	Red de enlace en el router con HE.	2001:470:1f06:239::1

Tabla 2.5 Puertas de enlaces predeterminadas para cada una de las redes que se encuentran en el Centro de Extensión Universitaria.

En este caso, la puerta de enlace para el router antares.udg.co.cu, sería la IP de la red de enlace del router externo (2001:470:1f06:239::1), conexión que se hace actualmente a través de un túnel con interfase SIT (anexo 2).

En el anexo 2, se muestra la configuración de la red para el router antares.udg.co.cu, esta información la contiene el archivo network, que se encuentra en el directorio /etc/sysconfig.

En el router – firewall del nodo principal (antares.udg.co.cu) será necesario entonces implementar una serie de rutas para garantizar la llegada de los paquetes provenientes de cualquiera de las redes, y con destino a las redes del campus universitario, para ello basta con especificar que todos los paquetes con destino a la red 2001:b00:f80b:200::/56 sean enviados al router con la dirección IP 2001:b00:f80b:3::2, a través del dispositivo o de la interfase SIT1 (Túnel de enlace IPV6 con la Universidad). (anexo 3). Note que el prefijo /56, incluye desde la red con prefijo /64, 2001:b00:f80b:200::/64 hasta la 2001:b00:f80b:2ff::/64.

Es importante destacar, que se aspira a lograr una conexión IPv6 nativa con el proveedor (RedUniv), sin necesidad del empleo de túneles, de manera que se puedan aprovechar al máximo todas las potencialidades que este novedoso protocolo brinda, cuando esto se logre, se ha previsto que el enlace IPv6 a Internet, sea a través del router principal de la institución (Cisco 2811), y no por medio del router – firewall antares.udg.co.cu. A partir de este momento, cambiarían las tablas de rutas de antares.udg.co.cu, pues la puerta de enlace predeterminada de éste, pasará a ser la dirección IP del router principal (2001:b00:f80b::1), también será necesario, especificar las rutas necesarias en éste de manera que se garantice el tráfico con las redes internas: primeramente será presiso indicar una ruta para todos los paquetes destinados a la red 2001:b00:f80b:1::/64, es decir, a la red interna de servidores del nodo Bayamo, para encaminar el tráfico a la red del Centro de Extensión Universitaria (2001:b00:f80b:4::/64), y finalmente otra ruta a la red del campus (2001:b00:f80b:200::/56), todas éstas, tendrán como puerta de enlace, la dirección IP del router antares.udg.co.cu (2001:b00:f80b::3).

Hasta aquí, hay que señalar, que es seguro el cambio de direcciones IPv6 cuando ocurra la conexión o enlace nativo a la red IPv6 externa o pública, pero se han utilizado las IP actuales como una manera de referirse a las interfases.

También será importante especificar una puerta de enlace para el router principal de la institución la cual será la IP del router del proveedor, en la red de enlace con el primero.

2.5 Configuración del protocolo IPv6 en routers, servidores y estaciones de trabajo.

2.5.1 Configuración de las interfases de red en los routers – firewall.

Uno de los primeros pasos, a la hora de instalar el protocolo IPv6 en cualquier red, será, la habilitación de éste en los routers de las diferentes redes existentes, en el caso de la red de la Universidad de Granma, solo es necesario la configuración de éste protocolo en los routers elektra.udg.co.cu, antares.udg.co.cu y Cisco 2811.

En los anexos 4A, 4B, 4C y 4D se exibe la configuración de las interfases de red para el caso del router – firewall elektra.udg.co.cu, estos se corresponden con los archivos de configuración de las interfases de red de este servidor, que se encuentran en el directorio /etc/sysconfig/networkscripts/, perteneciendo el archivo ifcfg-eth0, a la interfase de la red de los servidores del nodo, ifcfg-eth2 a la interfase de la red del área económica, el archivo ifcfg-eth3 a la interfase que se encuentra en la red pública y, finalmente, el archivo ifcfg-sit1, a la interfase SIT del túnel de enlace con el router antares.udg.co.cu.

En los anexos 5A, 5B, 5C, 5D y 5E, se aprecia la configuración de las interfases de red para el caso del router – firewall antares.udg.co.cu, estos se relacionan con los archivos de configuración de las interfases de red de este servidor, que se encuentran, al igual que en el caso anterior, en el directorio /etc/sysconfig/networkscripts/, donde pertenecen los archivo ifcfg-eth0, a la interfase de la red interna de los servidores del nodo, ifcfg-eth1 a la interfase de la red de la zona desmilitarizada, ifcfg-eth3 a la interfase que se encuentra en la red pública del Centro de Extensión Universitaria, ifcfg-sit1 al túnel de enlace entre los routers – firewall de los nodos de Bayamo y Universidad, y finalmente ifcfg-sit2, a la interfase de red del túnel de enlace del router antares.udg.co.cu con el router del proveedor temporal HE.

Hay que destacar que los servidores con Linux se configuraron para el soporte del protocolo IPv6 utilizando la misma metodología descrita anteriormente, pues los routers antares.udg.co.cu y elektra.udg.co.cu, son computadoras con sistema operativo Linux.

2.5.2 Configuración de las interfases de red para IPv6 en los servidores con sistema operativo Windows 2003.

Una vez instalado el protocolo IPv6 en éstos, solamente es necesario especificarles una configuración, de manera que no la adquieran automáticamente, por ello hay que asignarles una dirección IP, la puerta de enlace predeterminada y que no actúen como “Indicadores de Routers” (Router Advertisement). Esto se realizó con el comando “netsh”.

A continuación, se muestra de manera general la forma en que este comando fue utilizado.

c:\> netsh interface ipv6 add address "Local Area Connection" [direcciónIP] store=persistent

Con este primer comando, se le asigna una dirección IPv6 estática de manera persistente (cuando se reinicia la computadora no se pierde la IP), a la interfase "Local Área Connection" de una computadora con sistema operativo Windows XP (Service Pack II) o Windows 2003.

c:\> netsh interface ipv6 set interface "Local Area Connection" advertise=disabled store=persistent

Con éste se deshabilita la advertencia o indicación de router para la interfase "Local Área Connection"

c:\> netsh interface ipv6 add route ::/0 "Local Area Connection" nexthop=[IP puerta de enlace] publish=yes store=persistent

Finalmente se le asigna una puerta de enlace predeterminada a lPv6 del ordenador que se está configurando.

2.5.3 Configuración de los clientes. Asignación de direcciones IP dinámicas por radvd.

Tanto la asignación de direcciones IP a las estaciones de trabajo de una red con IPv6, como la información adicional necesaria que para el normal funcionamiento de este protocolo se requiere, puede hacerse de manera manual (estática), o automática (autoconfiguración). El método manual, descrito anteriormente para la asignación de configuraciones estáticas a los servidores (tanto Windows 2003 como Linux), en IPv6 tiende a ser un poco complejo, pues requiere que se especifiquen un conjunto de comandos o la edición de los archivos que contienen la configuración, por otra parte, el protocolo fue diseñado especialmente para la configuración automática. Con relación a esto, Palet (2006), considera que IPv6 es Plug & Play, pues el mismo se caracteriza por su elevada capacidad de autoconfiguración, lo cual no es mas que el conjunto de pasos por los cuales una estación de trabajo decide como configurar sus interfases en IPv6. Este autor alega que el proceso de autoconfiguración incluye la creación de una dirección de enlace local, verificación de que la misma no esté duplicada en dicho enlace y

determinación de la información que ha de ser autoconfigurada (direcciones de DNS, puertas de enlace, etc).

Según la Guía del Router IPv6 en Gentoo, para asignar direcciones a los clientes, la especificación IPv6 permite tanto la asignación con estado como sin estado (Gentoo Foundation, 2006).

El proyecto de esta investigación incluyó, desde sus inicios, la autoconfiguración con estado de las estaciones de trabajo de la red, pues se trata de una red muy extensa y con numerosas estaciones de trabajo, por lo que la configuración estática de cada una de las estaciones de trabajo resultaría extremadamente engorrosa.

El objetivo de utilizar DHCP se basaba en las facilidades de control de asignación que se puede tener con éste, tales como reservas, informaciones adicionales a suministrar a los clientes, etc; sin embargo, cuando se instaló el protocolo, se detectó que los ordenadores con Windows XP o Windows 2000, que representan el sistema operativo imperante en la red, no incluyen un DHCP cliente para IPv6, por lo que entonces, para emplear DHCP, habría que instalar en cada ordenador algún cliente, actividad esta que resultaría casi equivalente a configurar las estaciones de trabajo de manera estática o manual. Por ello, se valoró la variante de utilizar una configuración sin estado, empleando el servicio "Router Advertisement (radvd), cuando se emplea éste, configurar las máquinas es muy sencillo, solo precisa la conexión física a la red, y desde luego, que éstas tengan instalados el protocolo, además, tanto las estaciones de trabajo con sistema operativo Windows como Linux se encuentran habilitadas para su empleo.

EL Router Advertisement se instaló en los routers antares.udg.co.cu y elektra.udg.co.cu. En el anexo 7A, se muestra la configuración hecha para el primer router anteriormente mencionado, y en el anexo 7B, la configuración que se le asignó al segundo.

2.6 Implementación de cortafuegos con IP6Tables en los routers que lo requieran.

Según Linares (2005), un cortafuegos, es un dispositivo que funciona como un filtro entre dos o mas redes, permitiendo o denegando las transmisiones de paquetes de una red a la otra. Un uso típico es situarlo entre una red local y la red pública, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial.

Es importante destacar que el uso de cortafuegos, no se limita solamente al filtrado de paquetes entre las redes públicas y privadas, éstos se emplean también, y no con poca frecuencia, en filtrar el paso de paquetes, entre subredes pertenecientes a una misma

LAN o a una misma red privada, además, no siempre se destinan a controlar los datagramas que podrían pasar de una red a otra a través de una computadora, existen firewalls o cortafuegos mas sencillos que se instalan para proteger una computadora independiente, no una red; por ejemplo, el Personal Firewall, software para el sistema operativo Windows XP. En esta investigación resultarán de interés solamente los cortafuegos destinados a proteger o controlar el paso de una red a otra, utilizando una computadora que se halla en ambas redes, pues posee varias interfaces de red.

Es fácil percibir que los routers o enrutadores son equipos ideales para la creación de firewalls, de hecho, la mayoría de routers comerciales permiten su implementación. Si se analiza la anterior figura 2.4, puede notarse que todo el tráfico entre las diferentes subredes del campus universitario, se realiza a través del router elektra.udg.co.cu, de igual manera, el tráfico entre las diferentes subredes existentes en el Centro de Extensión Universitaria (figura 2.1), es, a través de la computadora antares.udg.co.cu; puede notarse también que todo el tráfico existente entre cualquier red del campus, con el nodo de Bayamo, las sedes universitarias o redes externas, siempre tendrán que pasar por ambos routers para llegar a cualquiera de las subredes del área universitaria.

De hecho, en estos dos servidores, existen cortafuegos para el protocolo IPv4, implementados con IPTables, sin embargo, a partir del momento en que se habilitó el IPv6 en la red, se hizo imprescindible la creación de algún tipo de filtrado de paquetes entre las diferentes subredes que garantizara un mínimo de seguridad, esto se logró instalando el IP6Tables en los routers elektra.udg.co.cu y antares.udg.co.cu.

El conjunto de reglas que se crearon, (basadas en IP6Tables), se muestran en los anexos 6A y 6B, donde el primero pertenece a las reglas implementadas para el firewall del nodo central (antares.udg.co.cu) y el segundo, para el firewall del nodo del campus universitario (elektra.udg.co.cu).

Explicar detalladamente, las reglas creadas con IP6Tables, harían este informe muy extenso, además, esto forma parte de otra investigación, por lo que solo se mencionarán los aspectos mas importantes y generales.

El tráfico de paquetes IPv6, proveniente de las redes internas de cualquiera de los dos nodos, es completamente abierto, esto quiere decir, que se permite el paso en ambos cortafuegos de los datagramas IPv6 que provengan de las redes 2001:b00:f80b:200::/64 o 2001:470:1f07:239::/64, y vayan con destino a cualquier otra subred.

En ambos firewalls o cortafuegos, se hace primeramente, una clasificación de los paquetes que pasan por éstos, en base a sus direcciones de origen, destino e interfases de salida reenviándose para que sean filtrados en dependencia de esto (figura 2.7).

```
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -d 2001:b00:f80b::/64 -o eth1 -j goodn-dmz
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -d 2001:b00:f80b::/64 -o eth1 -j intrn-dmz
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -d 2001:470:1f07:239::/64 -o eth0 -j intrn-goodn
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -d 2001:b00:f80b:4::/64 -o eth3 -j goodn-intrn
ip6tables -A FORWARD -s 2001:b00:f80b::/64 -d 2001:470:1f07:239::/64 -o eth0 -j dmz-goodn
ip6tables -A FORWARD -s 2001:b00:f80b::/64 -d 2001:b00:f80b:4::/64 -o eth0 -j dmz-intrn
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -d 2001:b00:f800::/44 -o eth1 -j goodn-rn
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -d 2001:b00:f800::/44 -o eth1 -j intrn-rn
ip6tables -A FORWARD -i sit1 -d 2001:b00:f80b::/64 -o eth1 -j univ-dmz
ip6tables -A FORWARD -i sit1 -d 2001:470:1f07:239::/64 -o eth0 -j univ-goodn
ip6tables -A FORWARD -i sit1 -d 2001:b00:f80b:4::/64 -o eth3 -j univ-intrn
ip6tables -A FORWARD -i sit1 -d 2001:b00:f800::/44 -o eth1 -j univ-rn
ip6tables -A FORWARD -i eth1 -s 2001:b00:f80b::/64 -o sit1 -j dmz-univ
ip6tables -A FORWARD -i eth0 -s 2001:470:1f07:239::/64 -o sit1 -j goodn-univ
ip6tables -A FORWARD -i eth3 -s 2001:b00:f80b:4::/64 -o sit1 -j intrn-univ
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -o sit2 -j goodn-bad
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -o sit2 -j intrn-bad
ip6tables -A FORWARD -i sit1 -o sit2 -j univ-bad
ip6tables -A FORWARD -i eth1 -d 2001:b00:f800::/44 -o sit1 -j rn-univ
ip6tables -A FORWARD -i eth1 -d 2001:b00:f800::/44 -o eth0 -j rn-goodn
ip6tables -A FORWARD -i eth1 -d 2001:b00:f800::/44 -o eth3 -j rn-intrn
ip6tables -A FORWARD -o sit1 -j bad-univ
ip6tables -A FORWARD -o eth0 -j bad-goodn
ip6tables -A FORWARD -o eth3 -j bad-intrn
#ip6tables -A FORWARD -j LOG --log-prefix "chain-jump "
ip6tables -A FORWARD -j DROP
```

Figura 2.7 Cadenas de saltos creadas en el firewall antares.udg.co.cu

En la figura anterior, puede notarse la manera que se agrupan los paquetes que intenten pasar a través del firewall antares.udg.co.cu. La primera línea indica que todos los paquetes provenientes de la red interna de los servidores del nodo de Bayamo, (todos los paquetes cuya dirección de origen sea la 2001:470:1f07:239::/64), y su destino sea la red de la zona desmilitarizada (-d 2001:b00:f80b::/64), utilizando para salir la interfase de red eth1 (-o eth1), serán enviados a las cadenas llamadas goodn-dmz.

Si los paquetes no se corresponden con las condiciones indicadas en la primera línea, entonces se compararán con las indicadas en la segunda, y así sucesivamente, hasta que llegue a la última, donde se les impedirá el paso sin notificación al emisor. (ip6tables -A FORWARD –j DROP).

El filtrado se hace de manera posterior al salto, por ejemplo, si un grupo de paquetes que intenta atravesar el router, cumplen con las condiciones especificadas en la segunda línea del anterior gráfico, entonces son reenviados al conjunto de cadenas de filtrado intrn-dmz; (Figura 2.8).

```
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::4/128 \
        -m multiport --dport http,ftp,ftp-data,domain -j ACCEPT
ip6tables -A intrn-dmz -p udp -d 2001:b00:f80b::4/128 --dport domain -j ACCEPT
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::4/128 --dport 1024:65535 -j ACCEPT
ip6tables -A intrn-dmz -p udp -d 2001:b00:f80b::4/128 --dport 1024:65535 -j ACCEPT
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::5/128 \
        -m multiport --dport http,ftp,ftp-data -j ACCEPT
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::5/128 --dport 1024:65535 -j ACCEPT
ip6tables -A intrn-dmz -p udp -d 2001:b00:f80b::5/128 --dport 1024:65535 -j ACCEPT
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::6/128 \
        -m multiport --dport http,ftp,ftp-data -j ACCEPT
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::6/128 --dport 1024:65535 -j ACCEPT
ip6tables -A intrn-dmz -p udp -d 2001:b00:f80b::6/128 --dport 1024:65535 -j ACCEPT
#ip6tables -A intrn-dmz -j LOG --log-prefix "intrn-dmz "
ip6tables -A intrn-dmz -j DROP
```

Figura 2.8. Reglas de filtrado establecidas para el flujo de datos provenientes de la red pública del Centro de Extensión Universitaria y con destino a la red o zona desmilitarizada.

Entonces, el firewall o cortafuegos irá comparando las direcciones IP de origen, destino, interfases de salida, puertos de origen, destino, etc, con cada una de las reglas especificadas, puede notar que para el caso del conjunto de reglas agrupadas bajo el nombre intrn-dmz, es decir, los paquetes que provienen de la red pública del Centro de Extensión Universitaria, y se dirigen a la red de la zona desmilitarizada, solo se permiten los paquetes IPv6 que cumplen con las condiciones siguientes:

1. protocolo TCP, con destino al host 2001:b00:f80b::4 y vaya dirigido a los puertos HTTP, HTTPS, TFP o DNS.
2. Que sea protocolo UDP, con destino al host 2001:b00:f80b::4 y el puerto de destino sea al de DNS (53).
3. Que sea protocolo TCP o UDP, para los puertos de destino desde el 1024 hasta el 65535 del host 2001:b00:f80b::4.
4. Se aplican reglas similares para el host 2001:b00:f80b::5, excluyendo las correspondientes al DNS, pues el anterior (2001:b00:f80b::4) es un servidor DNS, y el 2001:b00:f80b::5 no.
5. Se aplican reglas símilares para el 2001:b00:f80b::6 (jabber.udg.co.cu)

Se habilitara además, el protocolo ICMP para poder hacer pruebas de retroalimentación, conectividad, etc, entre las diferentes subnets existentes figura 2.9.

```
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type echo-request -j ACCEPT
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type ping -j ACCEPT
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type echo-reply -j ACCEPT
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT
# ip6tables -A icmp-acc -j LOG --log-prefix "icmpv6-acc "
# ip6tables -A icmp-acc -p icmpv6 -j ACCEPT
ip6tables -A icmp-acc -j DROP
```

Figura 2.9. Reglas para habilitar el protocolo ICMP en el router antares.udg.co.cu

2.7 Servidores de sistemas de nombres de dominio (DNS).

En la red de la Universidad de Granma existen cuatro servidores de nombres de dominio (DNS): uno externo, que se encuentra en la red de la zona desmilitarizada (mediaserver.udg.co.cu, 200.14.53.4 ó 2001:b00:f80b::4), y para el que se utiliza Bind, versión 9.3.4-P1, éste es el DNS en el que el proveedor ha delegado el control de las zonas pertenecientes al dominio de la institución, por ello, el que utiliza cualquier cliente externo para resolver direcciones, tanto directas como inversas de la red universitaria.

Este servidor se encuentra configurado con resolución de *varias vistas*, es decir, la forma de resolver, tanto direcciones IP como nombres de hosts, dependerá de la dirección IP de donde provenga la solicitud, se resuelve de una manera para las solicitudes provenientes de la red interna o de la red privada RedUniv, y de otra para las resultantes de la red pública externa (Internet).

La Figura siguiente (2.10), muestra la manera empleada para configurar las diferentes *vistas* en el servidor DNS externo, a través de listas de control de accesos (ACL) donde se destacan las dos vistas existentes. En esta figura, se puede deducir, que la declaración de las zonas, se hace en los archivos */etc/named.rfc1912.internal.zones*, para la vista interna, y */etc/named.rfc1912.external.zones.*

```
acl "trusted" {
10.0.0.0/8;
127.0.0.1;
200.14.48.0/21;
};

view internal-ir {
        match-clients { trusted; };
        recursion yes;
        include "/etc/named.rfc1912.internal.zones";
};

view external-ir {
        match-clients { any; };
        recursion yes;
        include "/etc/named.rfc1912.external.zones";
};
```

Figura 2.10. Configuración de un servidor DNS, con dos vistas, utilizando Bind.

Los anexos 8A y 8B, contienen, los archivos de declaración de zonas, el primero la información para la resolución de las zonas internas (*named.rfc1912.internal.zones*) y el segundo, para las externas (*named.rfc1912.internal.zones*). Podrá notar que la declaración de las zonas IPv6, se hace, fundamentalmente, para las zonas internas, pues, este servidor, de momento, no posee acceso a redes públicas con IPv6, es preciso recordar que el único segmento de red conectado a la red global con el protocolo antes mencionado, y que posee direcciones IP públicas "reales", es el de la red interna de los servidores del nodo (2001:470:1f07:239::/64), y no el de la zona desmilitarizada (2001:b00:f80b::/64)

Analizando estos anexos, se puede detectar que en ambos se configuró una zona de búsqueda para las resoluciones directas (cuando se intenta resolver una dirección IP a partir de un nombre), es decir, fue necesario declarar dos zonas de éste tipo, una para la vista interna y otra para la externa.

El anexo 9A muestra el archivo que almacena los datos de la zona de búsqueda directa, para la resolución o la vista externa, mientras que el anexo 9B refleja el archivo que contiene los registros de la zona de búsqueda directa para la vista interna, donde se destacan los registros del tipo AAAA que se utilizan para asignarle a un ordenador, una dirección IPv6.

El análisis de los anexos 8A y 8B, también indica que se declararon tantas zonas de búsqueda para las resoluciones inversas (cuando se desea resolver un nombre a partir de una dirección IP) como segmentos de red IPv6 existen en la institución, de ahí que resultaran declaradas 8 zonas de resolución inversa IPv6 para la vista interna del servidor DNS que se está describiendo, como se muestra en la tabla 2.6, donde podrá notarse también la manera de nombrar los archivos que contendrán los registros para la resolución inversa IPv6 de una zona determinada.

Dirección de red	Archivo de datos de la zona	Descripción
2001:b00:f80b::/64	0.0.0.0.b.0.8.f.0.0.b.0.1.0.0.2.ipv6.arpa	Red zona desmilitarizada
2001:470:1f07:239:: /64	9.3.2.0.7.0.f.1.0.7.4.0.1.0.0.2.ipv6.arpa	Red interna, servidores del nodo Bayamo.
2001:470:1f06:239:: /64	9.3.2.0.6.0.f.1.0.7.4.0.1.0.0.2.ipv6.arpa	Red de enlace con el proveedor IPv6 HE.
2001:b00:f80b:3::/64	3.0.0.0.b.0.8.f.0.0.b.0.1.0.0.2.ipv6.arpa	Red del túnel de enlace entre los nodos Universidad y Bayamo.
2001:b00:f80b:4::/64	4.0.0.0.b.0.8.f.0.0.b.0.1.0.0.2.ipv6.arpa	Red corporativa del Centro de Extensión Universitaria.
2001:b00:f80b:200::/64	0.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ipv6.arpa	Red de los servidores del nodo de la Universidad.
2001:b00:f80b:204::/64	4.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ipv6.arpa	Red corporativa del campus.
2001:b00:f80b:208::/64	8.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ipv6.arpa	Red el area económica.

Tabla 2.6 Zonas para la resolución inversa declaradas para la vista interna.

El anexo 10A muestra los registros existentes en el archivo de configuración de la zona inversa perteneciente a la red interna de los servidores del nodo Bayamo. Los anexos 10B y 10C, ofrecen los registros para la resolución inversa de las zonas pertenecientes a las redes del nodo Universitario y la red corporativa del campus, respectivamente.

Los tres servidores DNS restantes, con sistema operativo Windows 2003 y controladores de dominio primario con DNS, se encuentran, uno, en la red interna del nodo central de Bayamo (thot.udg.co.cu), otro en la red del nodo del campus universitario (hércules.udg.co.cu) y un tercero en la red corporativa de la Universidad (phraates.udg.co.cu).

La configuración para IPv6 de estos servidores de nombres, se realizó siguiendo una filosofía similar a la descrita anteriormente para las zonas de búsqueda directa e inversa de la vista interna, pero resultó muy sencilla por las facilidades de la interfaz gráfica que ofrecen la mayoría de las herramientas de Microsoft, incluso, solo fue necesario configurar uno de los DNS, pues, al estar éstos integrados al directorio activo, los cambios se replicaron automáticamente en el resto de los servidores.

Hay que señalar que el único DNS con soporte para IPv6, visible desde redes externas basadas en este protocolo, én estos momentos es el instalado en el controlador de dominio primario thot.udg.co.cu, por ello, es el que se está empleando para las resoluciones globales IPv6; el sistema de servidores DNS, está diseñado para una futura conexión nativa a redes externas IPv6 a través del router principal que se encuentra en la zona desmilitarizada, con el DNS externo que se ubica en esta red, cuya configuración fue descrita en detalle, de manera que los servidores de nombres internos, hagan consultas recursivas al DNS externo en caso de consultas para resoluciones a hosts que se salgan de la red privada, pero es útil recordar, que lo que se ha logrado hasta ahora, es una conexión a través de un túnel hecho con un proveedor remoto (HE) a través del router-firewall antares.udg.co.cu, quedando como red con IPv6 conectada a redes externas, y con direcciones públicas, la red en la que el controlador de dominio antes mencionado se encuentra, por este motivo, este fue el servidor que se declaró al proveedor HE para la delegación del control de zonas y se estableció como el servidor “forwarders” o servidor de reenvíos para el resto de los servidores de nombres de dominio. Cuando se logre una conexión a redes IPv6 oficial, con direcciones IP públicas asignadas por LACNIC, a través del proveedor de RedUniv, y usando para el enlace el router principal de la institución, entonces, el servidor primario será el externo (mediaserver.udg.co.cu), y el resto consultará a éste como servidor “forwarder”.

2.8 Rutas multicast, necesidad de su utilización.

El protocolo IPv6, se caracteriza, entre otros aspectos, por el soporte multicast de forma implícita o incluida, sin embargo, se pudo comprobar que cuando se utilizan túneles para encapsularlo en otro protocolo, (IPv4), con el objetivo de conectar varias redes, es preciso entonces implementar, los enrutamientos multicast.

En el caso de la red de la Universidad de Granma, fue necesario establecer rutas multicast, entre los nodos central de Bayamo y el nodo del campus universitario.

Por las características del enlace IPv6 existente entre el nodo central de Bayamo y el nodo del campus universitario, se hizo necesario configurar las rutas multicast en los enrutadores que los conectan: antares.udg.co.cu y elektra.udg.co.cu, para ello, se utilizó el MRD6, versión 0.9.6. Este es un software modular, creado precisamente con el objetivo de posibilitar rutas multicast en ruteadores con sistema operativo Linux.

En ambos routers, el código fuente de éste programa, se compiló empleando su configuración por defecto, y la instalación se efectuó en los directorios */usr/local/bin*, */usr/local/lib/mrd6/* y */usr/local/sbin*. La configuración se ubicó en el archivo */usr/local/sbin/mrd.conf*; en los anexos 11A y 11B, se muestra el contenido de los archivos mrd.conf, en los routers antares.udg.co.cu y elektra.udg.co.co, respectivamente, en éstos se destacan que se hace un registro completo del funcionamiento del proceso en el archivo */var/log/mrd6/mrd6.log*, se definen las rutas con el comando mrib, donde para el caso de las rutas de todo el tráfico dirigido a cualquiera de las redes ubicadas en el área del campus (2001:b00:f80b:200::/56), se envíe a través del la red del túnel, específicamente, a la IP del router elektra.udg.co.cu (2001:b00:f80b:3::2).

En este caso, los enrutamientos multicast fueron implementados utilizando PIM en modo disperso (PIM-SM), para ello se definió un grupo multicast, el ff1e::/16, esto requiere un *punto de encuentro* (Rendezvous point, RP) que constituirá la dirección IP del router principal (antares.udg.co.cu) que se corresponde con la red en la que se encuentra el emisor de una transmisión multicast (2001:470:1f07:239::1); es notable el hecho de que el punto de encuentro, ubicado en la red interna de los servidores del nodo de Bayamo, limita las rutas multicast a las comunicaciones entre toda la red del campus universitario y red interna de servidores del nodo central de Bayamo, pero hay que aclarar que esto es algo experimental, que aún no supera el período de pruebas, por ello, en un futuro, pueden crearse otros grupos que faciliten las transmisiones multicast entre las diferentes redes públicas existentes.

En el anexo 11B, pueden apreciarse las rutas definidas y el grupo multicast, con el punto de reunión señalando también a la dirección 2001:470:1f07:239::1.

2.9 Configuración de algunos servicios y aplicaciones sobre IPv6. WWW, FTP y Jabber.

Actualmente, existen en la universidad los sitios web oficiales:

- Portal externo (www.udg.co.cu), con Internet Information Service corriendo en un sistema operativo Windows 2003 con Service Pack 2, host: mail.udg.co.cu.
- Portal web de la Intranet (intranet.udg.co.cu) con Apache 2.2, en un sistema operativo Fedora Core 6 con nombre intranet.udg.co.cu.
- El sitio de la biblioteca: ict.udg.co.cu, montado con Internet Information Service en un Windows 2003.

En ninguno de estos fue necesario habilitar una configuración especial para el soporte IPv6, pues todos comenzaron a responder a las solicitudes Web entrantes con el protocolo mencionado, esto pudo comprobarse, revisando los registros de accesos al servidor.

El acceso al servicio de correos en la institución, se hace a través de un cliente Web que el mismo servidor trae incorporado y que aún no soporta IPv6, por ello, su acceso, aún es utilizando solamente el protocolo IPv4.

Existen también otros servicios webs secundarios, tales como los que se encuentran en los servidores proxy.udg.co.cu, proxy1.udg.co.cu, jabber.udg.co.cu, entre otros, ocurriendo de igual manera, una vez habilitado el protocolo IPv6, éstos comenzaron a responder tanto a las solicitudes entrantes con IPv4, como a las hechas con protocolo IPv6.

Es preciso aclarar que la interfase de configuración del Internet Information Services no admite configuraciones para IPv6, solo IPv4, pero esto no constituye un obstáculo para el soporte de este protocolo por parte del Software.

FTP:

Es preciso aclarar que los servidores implementados con Internet Informations Service, solo soportan IPv6 para el servicio WWW, los servicios FTP (protocolo de transferencia de ficheros), SMTP (protocolo de transferencia simple de correos), y NNTP (protocolo de transferencia de noticias) no son soportados aún.

El servidor FTP de la intranet, se basa en el software Very Segurity FTP, este si fué configurado con soporte para el protocolo IPv6.

JABBER:

El servidor jabber de la institución, se encuentra en el host jabber.udg.co.cu, se utiliza el jabberd, versión 1.4.4, el mismo fue compilado con soporte para ambas versiones del protocolo IP.

2.10 Conclusiones del capítulo.

En este capítulo se ha hecho una descripción detallada de los pasos que se siguieron para la instalación del protocolo IPv6 en la Universidad de Granma y se puede concluir el mismo afirmando que el protocolo se encuentra instalado en las redes que forman el nodo central de Bayamo, la red corporativa del Centro de Extensión Universitaria, la red de los servidores del nodo del campus universitario, y la red corporativa del campus, en la que se encuentran mas del 60% de las estaciones de trabajo, además, queda conectada a la red externa y pública IPv6, la red interna de los servidores del nodo central de Bayamo, es preciso estudiar en un futuro, el comportamiento del servidor proxy Squid con soporte IPv6, para poder dar servicios de acceso a redes externas basadas en este protocolo, esto se debe a que la única red que tiene direcciones IP públicas, y reconocidas es la interna del nodo de Bayamo.

3 Conclusiones finales.

- Se logró instalar el protocolo IPv6 en la mayoría de las sub redes pertenecientes a la red informática de la Universidad de Granma.
- Fue superada la principal barrera tecnología que impedía la instalación de este protocolo, la cual consistía, en la limitación para las comunicaciones IPv6 entre los dos nodos universitarios, por falta de soporte del proveedor y los enrutadores existentes.
- Todos los pasos seguidos durante la instalación del protocolo IPv6, se documentaron detalladamente de manera que este documento pueda ser utilizado como una guía para quienes deseen utilizar este protocolo en las redes de sus respectivas entidades.
- Se ofrece una vía alternativa para la conexión a redes públicas, globales o externas que utilicen el protocolo IPv6, mediante el empleo de túneles, quedando, a modo de ejemplo y futuros estudios, la red interna de los servidores del nodo de Bayamo, conectada y con acceso a servidores externos que soportan este protocolo, utilizando para ello un servidor público externo.

4 Recomendaciones.

- Continuar extendiendo el protocolo IPv6 a las redes que aún carecen de éste, tales como las de las Sedes Universitarias Municipales y el futuro laboratorio de Profesores.
- Estudiar la posibilidad del empleo de herramientas que sirvan para celebrar video conferencias basadas en IPv6.
- Realizar investigaciones posteriores sobre el uso de un Proxy que soporte el protocolo IPv6, de manera que pueda ser utilizado en una red con características similares a la del objeto de ésta investigación, de forma que se pueda dar acceso a redes externas IPv6 a las estaciones de trabajo de la red corporativa.
- Profundizar en los diferentes aspectos de las configuraciones que fueron hechas en los servidores, para optimizarlas y mejorarlas.
- Evaluar en futuros estudios, el comportamiento de la conexión a la red pública IPv6 utilizándo túneles SIT y el suministrador HE.

5 Referencias Bibliográficas.

Alcantara, A. F. (2003). IPv6: avances, mitos y perspectivas. Paper presented at the IPv6, Universidad Nacional Autonoma de Mexico.

Aldo, N., Gabriel, P., y Mariano, S. (2006). Arquitectura TCP/IP. Disponible en: http://web.frm.utn.edu.ar/comunicaciones/tcp_ip.html#1.7 [2007, Diciembre].

Alfonso, J. M. (2006). IPv6 en Cuba; estado actual y perspectivas. LACNICIX. Disponible en: http://www.lacnic.net/jesus-martinez-ipv6tf-cuba.pdf [2007, Diciembre].

Altes, J., y Serra, X. H. (2002). Análisis de Redes y Sistemas de Comunicaciones (UPC ed.).

Atelin, P., y Dordoigne, J. (2002). tcp/ip y protocolos de internet (2 Edicion ed.).

Atkinson, R. (1998). Normas RFC. Seguridad en la arquitectura del protocolo de internet (Noviembre). Disponible [2007, Noviembre].

Behrouz, F. (2006). Redes de comunicacion (McGraw-Hill ed.).

Black, U. (1999). Tecnologias Emergentes para Redes de Computadoras (Prentice Hall Hispanoamerica S.A. ed.). Mexico.

Cambronero, D. F. (2001). Introduccion al Protocolo IPV6.

Castañeda, R., López, M., y Servín, A. (2007). Arquitectura de IP Multicast para backbone de Internet 2 en México., 20. Disponible.

Castorina, E. D. (2004). Multicast. RNP. Disponible en: http://www.rnp.br/es/multicast/sobre.html [2007, Diciembre].

Deering, S. (1998). Internet Protocol, Version 6 (IPv6) Specification. Disponible en: http://www.ietf.org/rfc/rfc2460.txt [2007, Diciembre].

Finlayson, E., Mann, T., Mogul, H., y Theimer, M. (1984, June). A Reverse Address Resolution Protocol. Disponible en: http://tools.ietf.org/html/rfc903 [2007, Diciembre].

Gai, S. (1998). Internetworking IPv6 with Cisco Routers (Mcgraw Hill ed.).

García B, L. (2003). Sistemas distribuidos. Disponible en: http://www.udlap.mx/~genoveva/is417/FOLIEN/THEMA2/Repaso%20de%20redes.ppt.

Gartner, G. (2006). Realidad de las empresas. Disponible en: http://es.transnationale.org/empresas/gartner_group.php [2007, Diciembre].

Gentoo Foundation, I. (2006). Guia del router IPv6 en Gentoo. Disponible en: http://www.gentoo.org.

Gonzalez, J. M. (2005). IPv6 el protocolo primera aproximacion. I, 54. Disponible.

Guenul, O. (2005). Las Redes Wan. Disponible en: http://www.monografias.com/trabajos5/redwan/redwan.shtml.

Hagen, S. (2002). IPv6 Essentials (O'Reilly & Associates ed. Vol. I).

Hernández, M. J. D. V. (2006). IP versión 6 La nueva Generación de Internet. Disponible.

IEEE802. (1998). Estandar para informacion tecnologica. Disponible en: http://standards.ieee.org/getieee802/802.2.html [2007, Diciembre].

IETF. (1992). IETF. Disponible en: http://www.ietf.org/.

Johanson, P. (2006). Guía del router IPv6 en Gentoo (Camille Huot). Gentoo Foundation, Inc. Disponible en: http://www.GentooLinuxGuiadelrouterIPv6Gentoo.htm [2007, diciembre].

Kent, S., y Atkinson, R. (1998). IP Encapsulating Security Payload Request for Comments: 2406, 22. Disponible.

Lankenau, D., y Garza, C. (2007). Lotus Notes. Disponible en: http://www.mty.itesm.mx/rectoria/dda/usols/concepto1.htm [2007, 30/IX].

Linares, M. (2005). Cortafuegos. Paper presented at the Curso de Administración de redes, Universidad del Sur de Manabí.

Linares, M. (2007). Mapas conceptuales para la enseñanza de la Botánica. Una propuesta organizativa., Universidad Central “Martha Abreu”.

Lockhart, A. (2007). tuneles. 2007. Disponible en: http://www.textoscientificos.com/redes/redes-virtuales/tuneles [2008, enero].

Maigron, P. (2008). Regional Internet Registries Statistics. RIR Delegations & RIPE NCC Allocations. Disponible en: http://www-public.int-evry.fr/~maigron/RIR_Stats/index.html2008].

McPherson, D., y Halabi, S. (2002). Arquitecturas de enrutamiento en internet (2001 ed.).

Moreno, L. (2003). Tipos de redes. Disponible en: http://www.htmlweb.net/redes/topologia/topologia_1.htm.

NA. (2007a). Multidifusión. WIKIPEDIA La Enciclopedia Libre, España Disponible en: http://es.wikipedia.org/wiki/IP_Multicast [2007, Diciembre].

NA. (2007b). Protocolo de internet version 5. WIKIPEDIA La Enciclopedia Libre, España. Disponible en: http://es.wikipedia.org/wiki/IPv5 [2007, Diciembre].

Naranjo, A. (1997). Redes de Computadores. Disponible en: http://www.monografias.com/trabajos5/redes/redes.shtml.

Palet, J. (2003). Euro6IX: Primera Red IPV6 Europea. Disponible en: http://www.RedIRIS - Euro6IX Primera red IPv6 europea - _ Euro6IX European IPv6 Internet Exchanges Backbone.htm [2007, 22-XI-2007].

Palet, J. (2006). Tutorial de IPv6. Disponible [2008, Enero].

Peralta, L. (2002). IPv6. UJI, I, 1-36. Disponible.

Plumer, D. C. (1982). Un protocolo para la resolución de dirección Ethernet. Disponible en: http://www.rfc-es.org/rfc/rfc0826-es.txt.

Rengifo, F. (2004). Topologías para Redes. Disponible en: http://www.monografias.com/trabajos15/topologias-neural/topologias-neural.shtml.

Sanlés, C. D., y Vaamonde, M. D. F. (2003). Implementación de IPv6, QoS e IPSec con Linux. Disponible en: http://www.davidfv.net/articulos/trabajo_redes.pdf [2008, enero].

Sedano, J. (2001). Mundo Linux. Revistas Profesionales Linux, 6. Disponible.

Senso, J. (1996). IPV6: un respiro para la internet El profesional de la informacion. Disponible.

Soto, M. (2006). Protocolos TCP/IP, [Sitio Web]. Disponible en: http://www.sortorama.es/usuarios-lycos-es-janjo-janjo1-22456.html [2007.

Tanenbaum, A. (1996). Redes de Ordenadores (2da. Edicion ed.). Mexico.

Ureña-Poirier, H. D., y Martín, J. R. (2005). Montaje y configuración de una LAN. Disponible en: http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/ip.htm [2007, 21/11/2007].

Van-Beijnum, I. (2005). Running IPv6 (2 Edicion ed.).

Villa, J. (2004). IPV6 La Nueva Version de Internet. Grupo de Trabajo IPv6 Cuba, 57. Disponible.

6 Anexos.

Anexo 1. Configuración de la red en el servidor elektra.udg.co.cu (archivo: /etc/sysconfig/network)

```
NETWORKING=yes
HOSTNAME=elektra.udg.co.cu
GATEWAYDEV=eth1
FORWARD_IPV4=yes
DOMAINNAME=udg.co.cu
GATEWAY=192.168.251.1
NETWORKING_IPV6=yes
IPV6FORWARDING=yes
IPV6_AUTOCONF=yes
IPV6_AUTOTUNNEL=no
IPV6_DEFAULTGW="2001:0b00:f80b:3::1%sit1"
```

Anexo 2. Configuración de la red en el servidor antares.udg.co.cu (archivo: /etc/sysconfig/network)

```
NETWORKING=yes
HOSTNAME=antares.udg.co.cu
FORWARD_IPV4=yes
DOMAINNAME=udg.co.cu
NETWORKING_IPV6=yes
IPV6FORWARDING=yes
IPV6_AUTOCONF=no
IPV6_AUTOTUNNEL=no
IPV6_DEFAULTGW="2001:470:1f06:239::1%sit2"
```

Anexo 3. Rutas a especificar en el router – firewall antares.udg.co.cu. (Archivo: /etc/sysconfig/networkscripts/route6-sit1/)

```
2001:b00:f80b:200::0/56 via 2001:b00:f80b:3::2 dev sit1
```

Anexo 4A. Configuración de la red en el router elektra.udg.co.cu, interfase de red eth0 (Archivo /etc/sysconfig/networkscripts/ifcfg-eth0)

```
# VIA Technologies, Inc. VT6102 [Rhine-II]
DEVICE=eth0
BROADCAST=10.24.1.255
HWADDR=00:50:BA:0B:CC:04
IPADDR=10.24.1.1
IPV6ADDR=2001:b00:f80b:200::1
IPV6PREFIX=64
NETMASK=255.255.255.0
NETWORK=10.24.1.0
ONBOOT=yes
BOOTPROTO=static
IPV6INIT=yes
IPV6AUTOCONF=no
```

Anexo 4B. Configuración de la red en el router elektra.udg.co.cu, interfase de red eth2 (Archivo /etc/sysconfig/networkscripts/ifcfg-eth2)

```
# Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
DEVICE=eth2
ONBOOT=yes
BOOTPROTO=static
BROADCAST=192.168.4.255
HWADDR=00:48:54:65:F9:FB
IPADDR=192.168.4.1
IPV6ADDR=2001:b00:f80b:208::1
IPV6PREFIX=64
NETMASK=255.255.255.0
NETWORK=192.168.4.0
IPV6INIT=yes
IPV6AUTOCONF=no
```

Anexo 4C. Configuración de la red en el router elektra.udg.co.cu, interfase de red eth3 (Archivo /etc/sysconfig/networkscripts/ifcfg-eth3)

```
# Intel Corporation 82557/8/9 [Ethernet Pro 100]
DEVICE=eth3
BROADCAST=10.24.7.255
HWADDR=00:B0:D0:AA:EC:58
IPADDR=10.24.6.1
IPV6ADDR=2001:b00:f80b:204::1
IPV6PREFIX=64
NETMASK=255.255.254.0
NETWORK=10.24.6.0
ONBOOT=yes
IPV6INIT=yes
IPV6AUTOCONF=no
```

Anexo 4D. Configuración de la red en el router elektra.udg.co.cu, interfase de red sit1 (Archivo /etc/sysconfig/networkscripts/ifcfg-sit1)

```
DEVICE=sit1
IPV6INIT=yes
ONBOOT=yes
BOOTPROTO=static
IPV6ADDR=2001:0b00:f80b:3::2/64
IPV6AUTOCONF=no
IPV6TUNNELIPV4=192.168.250.2
IPV6TUNNELIPV4LOCAL=192.168.251.2
```

Anexo 5A. Configuración de la red en el router antares.udg.co.cu, interfase de red eth0 (Archivo /etc/sysconfig/networkscripts/ifcfg-eth0)

```
# Broadcom Corporation NetXtreme BCM5702X Gigabit Ethernet
DEVICE=eth0
BOOTPROTO=none
BROADCAST=200.14.53.31
HWADDR=00:0E:7F:FF:AC:AF
IPADDR=200.14.53.17
IPV6ADDR=2001:470:1f07:239::1/64
IPV6INIT=yes
IPV6AUTOCONF=no
NETMASK=255.255.255.240
NETWORK=200.14.53.16
ONBOOT=yes
TYPE=Ethernet
```

Anexo 5B. Configuración de la red en el router antares.udg.co.cu, interfase de red eth1 (Archivo /etc/sysconfig/networkscripts/ifcfg-eth1)

```
# Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
DEVICE=eth1
ONBOOT=yes
BOOTPROTO=none
IPADDR=200.14.53.3
NETMASK=255.255.255.248
GATEWAY=200.14.53.1
BROADCAST=200.14.53.7
HWADDR=00:30:4F:27:f0:39
IPV6ADDR=2001:b00:f80b::3/64
IPV6INIT=yes
IPV6AUTOCONF=no
NETWORK=200.14.53.0
TYPE=Ethernet
```

Anexo 5C. Configuración de la red en el router antares.udg.co.cu, interfase de red eth3 (Archivo /etc/sysconfig/networkscripts/ifcfg-eth3)

```
# Realtek Semiconductor Co., Ltd. RTL-8139/8139C/8139C+
DEVICE=eth3
BOOTPROTO=none
BROADCAST=10.24.100.255
HWADDR=00:30:4f:27:cf:55
IPADDR=10.24.100.1
NETMASK=255.255.255.0
NETWORK=10.24.100.0
ONBOOT=yes
TYPE=Ethernet
IPV6ADDR=2001:b00:f80b:4::1/64
IPV6INIT=yes
IPV6AUTOCONF=no
```

Anexo 5D. Configuración de la red en el router antares.udg.co.cu, interfase de red sit1 (Archivo /etc/sysconfig/networkscripts/ifcfg-sit1)

```
DEVICE=sit1
IPV6INIT=yes
ONBOOT=yes
BOOTPROTO=none
IPV6ADDR=2001:0b00:f80b:0003::1/64
IPV6AUTOCONF=no
IPV6TUNNELIPV4=192.168.251.2
IPV6TUNNELIPV4LOCAL=192.168.250.2
```

Anexo 5E. Configuración de la red en el router antares.udg.co.cu, interfase de red sit2 (Archivo /etc/sysconfig/networkscripts/ifcfg-sit2)

```
DEVICE=sit2
IPV6INIT=yes
ONBOOT=yes
BOOTPROTO=none
IPV6ADDR=2001:470:1f06:239::2/64
IPV6AUTOCONF=no
IPV6TUNNELIPV4=209.51.161.14
IPV6TUNNELIPV4LOCAL=200.14.53.3
```

Anexo 6A. Script para la creación de las reglas del cortafuegos en IP6Tables en el router antares.udg.co.cu (Archivo /iptables/ip6tables)

```
iptables -F INPUT
ip6tables -F FORWARD
ip6tables -F OUTPUT

ip6tables -A INPUT -j DROP
ip6tables -A FORWARD -j DROP
ip6tables -A OUTPUT -j DROP

# [goodn] eth0 - Red interna de servidores 2001:470:1f07:239::/64
# [intrn] eth3 - Red externa 2001:b00:f80b:4::/64
# [dmz] eth1 - Red de IP reales 2001:b00:f80b::/64

ip6tables -N univ-rn
ip6tables -N rn-univ
ip6tables -N goodn-rn
ip6tables -N rn-goodn
ip6tables -N ppp-rn
ip6tables -N rn-ppp
ip6tables -N intrn-rn
ip6tables -N rn-intrn
ip6tables -N ppp-bad
ip6tables -N bad-ppp
ip6tables -N goodn-dmz
ip6tables -N dmz-goodn
ip6tables -N intrn-dmz
ip6tables -N dmz-intrn
ip6tables -N dmz-univ
ip6tables -N univ-goodn
```

```
ip6tables -N goodn-univ
ip6tables -N univ-intrn
ip6tables -N intrn-univ
ip6tables -N goodn-bad
ip6tables -N bad-goodn
ip6tables -N intrn-bad
ip6tables -N bad-intrn
ip6tables -N univ-dmz
ip6tables -N univ-bad
ip6tables -N bad-univ
ip6tables -N ppp-univ
ip6tables -N univ-ppp
ip6tables -N ppp-intrn
ip6tables -N intrn-ppp
ip6tables -N intrn-goodn
ip6tables -N goodn-intrn
ip6tables -N ppp-dmz
ip6tables -N dmz-ppp
ip6tables -N intrn-good
ip6tables -N good-intrn
ip6tables -N icmp-acc

ip6tables -A FORWARD -m state --state INVALID -j DROP
ip6tables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

###############
# Chain jumps #
###############

ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -d 2001:b00:f80b::/64 -o
eth1 -j goodn-dmz
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -d 2001:b00:f80b::/64 -o
eth1 -j intrn-dmz
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -d 2001:470:1f07:239::/64 -o
eth0 -j intrn-goodn
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -d 2001:b00:f80b:4::/64 -o
eth3 -j goodn-intrn
ip6tables -A FORWARD -s 2001:b00:f80b::/64 -d 2001:470:1f07:239::/64 -o
eth0 -j dmz-goodn
ip6tables -A FORWARD -s 2001:b00:f80b::/64 -d 2001:b00:f80b:4::/64 -o
eth0 -j dmz-intrn
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -d 2001:b00:f800::/44 -o
eth1 -j goodn-rn
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -d 2001:b00:f800::/44 -o
eth1 -j intrn-rn
ip6tables -A FORWARD -i sit1 -d 2001:b00:f80b::/64 -o eth1 -j univ-dmz
ip6tables -A FORWARD -i sit1 -d 2001:470:1f07:239::/64 -o eth0 -j univ-
goodn
ip6tables -A FORWARD -i sit1 -d 2001:b00:f80b:4::/64 -o eth3 -j univ-
intrn
ip6tables -A FORWARD -i sit1 -d 2001:b00:f800::/44 -o eth1 -j univ-rn
ip6tables -A FORWARD -i eth1 -s 2001:b00:f80b::/64 -o sit1 -j dmz-univ
ip6tables -A FORWARD -i eth0 -s 2001:470:1f07:239::/64 -o sit1 -j goodn-
univ
ip6tables -A FORWARD -i eth3 -s 2001:b00:f80b:4::/64 -o sit1 -j intrn-
univ
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -o sit2 -j goodn-bad
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -o sit2 -j intrn-bad
```

```
ip6tables -A FORWARD -i sit1 -o sit2 -j univ-bad
ip6tables -A FORWARD -i eth1 -d 2001:b00:f800::/44 -o sit1 -j rn-univ
ip6tables -A FORWARD -i eth1 -d 2001:b00:f800::/44 -o eth0 -j rn-goodn
ip6tables -A FORWARD -i eth1 -d 2001:b00:f800::/44 -o eth3 -j rn-intrn
ip6tables -A FORWARD -o sit1 -j bad-univ
ip6tables -A FORWARD -o eth0 -j bad-goodn
ip6tables -A FORWARD -o eth3 -j bad-intrn
#ip6tables -A FORWARD -j LOG --log-prefix "chain-jump "
ip6tables -A FORWARD -j DROP

ip6tables -A icmp-acc -p icmpv6 --icmpv6-type echo-request -j ACCEPT
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type ping -j ACCEPT
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type echo-reply -j ACCEPT
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT
# ip6tables -A icmp-acc -j LOG --log-prefix "icmpv6-acc "
# ip6tables -A icmp-acc -p icmpv6 -j ACCEPT
ip6tables -A icmp-acc -j DROP

#######################################################
#### Fin de las Chain Jumps [Cadenas de Saltos] ####
#######################################################

############################
### Reglas de Filtrado ###
############################

# desde la red de los servidores del nodo a la zona desmilitarizada
goodn-dmz
# ip6tables -A goodn-dmz -j LOG --log-prefix "goodn-dmz "
ip6tables -A goodn-dmz -j ACCEPT

# Desde la Universidad a la red nacional
# ip6tables -A univ-rn -j LOG --log-prefix "univ-rn "
ip6tables -A univ-rn -j ACCEPT

# Desde la red de los servidores de Bayamo a la Red Nacional
# Se deja pasar todo
# ip6tables -A goodn-rn -j LOG --log-prefix "goodn-rn "
ip6tables -A goodn-rn -j ACCEPT

# Desde la red de la sede de Bayamo a la Red Nacional
# Se deja pasar todo
# ip6tables -A intrn-rn -j LOG --log-prefix "intrn-rn "
ip6tables -A intrn-rn -j ACCEPT

# desde la universidad a la zona desmilitarizada univ-dmz
# desde la red de los servidores de la universidad
ip6tables -A univ-dmz -s 2001:b00:f80b:200::/64 -j ACCEPT
ip6tables -A univ-dmz -s 2001:b00:f80b:3::2/128 -j ACCEPT

ip6tables -A univ-dmz -p tcp \
        -m multiport --dport 22,23,3389 -j DROP

# desde el servidor que esta en la intranet
ip6tables -A univ-dmz -s 2001:b00:f80b:204::2/128 -j ACCEPT
ip6tables -A univ-dmz -s 2001:b00:f80b:204::8/128 -j ACCEPT

ip6tables -A univ-dmz -p tcp -d 2001:b00:f80b::2/128 \
```

```
          -m multiport --dport http,ftp,ftp-data -j ACCEPT

ip6tables -A univ-dmz -p tcp -d 2001:b00:f80b::4/128 \
        -m multiport --dport http,ftp,ftp-data,domain -j ACCEPT
ip6tables -A univ-dmz -p udp -d 2001:b00:f80b::4/128 --dport domain -j
ACCEPT
ip6tables -A univ-dmz -p tcp -d 2001:b00:f80b::4/128 --dport 1024:65535 -
j ACCEPT
ip6tables -A univ-dmz -p udp -d 2001:b00:f80b::4/128 --dport 1024:65535 -
j ACCEPT

ip6tables -A univ-dmz -p tcp -d 2001:b00:f80b::5/128 \
        -m multiport --dport http,ftp,ftp-data -j ACCEPT
ip6tables -A univ-dmz -p tcp -d 2001:b00:f80b::5/128 --dport 1024:65535 -
j ACCEPT
ip6tables -A univ-dmz -p udp -d 2001:b00:f80b::5/128 --dport 1024:65535 -
j ACCEPT

ip6tables -A univ-dmz -p tcp -d 2001:b00:f80b::6/128 \
        -m multiport --dport http,ftp,ftp-data -j ACCEPT
ip6tables -A univ-dmz -p tcp -d 2001:b00:f80b::6/128 --dport 1024:65535 -
j ACCEPT
ip6tables -A univ-dmz -p udp -d 2001:b00:f80b::6/128 --dport 1024:65535 -
j ACCEPT

#ip6tables -A univ-dmz -j LOG --log-prefix "univ-dmz "
ip6tables -A univ-dmz -j DROP

# desde la red corporativa del nodo a la zona desmilitarizada intrn-dmz
ip6tables -A intrn-dmz -p tcp \
        -m multiport --dport 22,23,3389 -j DROP
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::2/128 \
          -m multiport --dport http,ftp,ftp-data -j ACCEPT

ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::4/128 \
        -m multiport --dport http,ftp,ftp-data,domain -j ACCEPT
ip6tables -A intrn-dmz -p udp -d 2001:b00:f80b::4/128 --dport domain -j
ACCEPT
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::4/128 --dport 1024:65535
-j ACCEPT
ip6tables -A intrn-dmz -p udp -d 2001:b00:f80b::4/128 --dport 1024:65535
-j ACCEPT

ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::5/128 \
        -m multiport --dport http,ftp,ftp-data -j ACCEPT
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::5/128 --dport 1024:65535
-j ACCEPT
ip6tables -A intrn-dmz -p udp -d 2001:b00:f80b::5/128 --dport 1024:65535
-j ACCEPT

ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::6/128 \
        -m multiport --dport http,ftp,ftp-data -j ACCEPT
ip6tables -A intrn-dmz -p tcp -d 2001:b00:f80b::6/128 --dport 1024:65535
-j ACCEPT
ip6tables -A intrn-dmz -p udp -d 2001:b00:f80b::6/128 --dport 1024:65535
-j ACCEPT

#ip6tables -A intrn-dmz -j LOG --log-prefix "intrn-dmz "
```

```
ip6tables -A intrn-dmz -j DROP

# Entradas
#ip6tables -A dmz-goodn -p tcp -d 2001:b00:f80b:1::3/128 -m multiport --
dport domain,ntp -j ACCEPT
#ip6tables -A dmz-goodn -p udp -d 2001:b00:f80b:1::3/128 -m multiport --
dport domain,ntp -j ACCEPT

ip6tables -A dmz-goodn -p tcp -d 2001:b00:f80b:1::3/128 \
       -m multiport --dport 42,53,88,123,135,137,139,389,445,636 -j
ACCEPT
ip6tables -A dmz-goodn -p udp -d 2001:b00:f80b:1::3/128 \
       -m multiport --dport 42,53,88,123,135,137,138,389,445,636 -j
ACCEPT
ip6tables -A dmz-goodn -p tcp -d 2001:b00:f80b:1::2/128 \
    -m multiport --dport smtp,pop3,imap,imap3,http,https,ntp -j ACCEPT
ip6tables -A dmz-goodn -p tcp \
    -m multiport --dport http,https,ftp,ftp-data,ntp,ldap -j ACCEPT
ip6tables -A dmz-goodn -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A dmz-goodn -p udp --dport 1024:65535 -j ACCEPT

# Salidas
ip6tables -A dmz-goodn -p tcp ! --syn --sport http -j ACCEPT
ip6tables -A dmz-goodn -p tcp ! --syn --sport https -j ACCEPT
ip6tables -A dmz-goodn -p tcp ! --syn --sport ftp -j ACCEPT
ip6tables -A dmz-goodn -p tcp ! --syn --sport ftp-data -j ACCEPT
ip6tables -A dmz-goodn -p tcp ! --syn --sport domain -j ACCEPT
ip6tables -A dmz-goodn -p tcp ! --syn --sport 1024: -j ACCEPT

ip6tables -A dmz-goodn -p icmpv6 -j icmp-acc
#ip6tables -A dmz-goodn -j LOG --log-prefix "dmz-goodn "
ip6tables -A dmz-goodn -j DROP

# desde la zona desmilitarizada a la red la red corporativa del nodo dmz-
intrn

ip6tables -A dmz-intrn -p tcp ! --syn --sport http -j ACCEPT
ip6tables -A dmz-intrn -p tcp ! --syn --sport ftp -j ACCEPT
ip6tables -A dmz-intrn -p tcp ! --syn --sport ftp-data -j ACCEPT
ip6tables -A dmz-intrn -p tcp ! --syn --sport domain -j ACCEPT
ip6tables -A dmz-intrn -p udp --dport domain -j ACCEPT
ip6tables -A dmz-intrn -p tcp ! --syn --sport 1024:65535 -j ACCEPT
ip6tables -A dmz-intrn -p tcp ! --syn --sport 1024:65535 -j ACCEPT
#ip6tables -A dmz-intrn -j LOG --log-prefix "dmz-intrn "
ip6tables -A dmz-intrn -j DROP

# Desde la red nacional a la Universidad completa
ip6tables -A rn-univ -p tcp \
       -m multiport --dport smtp,pop3,imap,imap3,http,https,ftp,ftp-
data,domain -j ACCEPT
ip6tables -A rn-univ -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A rn-univ -p udp --dport domain -j ACCEPT
ip6tables -A rn-univ -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A rn-univ -p icmpv6 -j icmp-acc
ip6tables -A rn-univ -j DROP

# Desde la Red Nacinal a la red del nodo bayamo
ip6tables -A rn-goodn -p tcp \
```

```
        -m multiport --dport smtp,pop3,imap,imap3,http,https,ftp,ftp-
data,domain -j ACCEPT
ip6tables -A rn-goodn -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A rn-goodn -p udp --dport domain -j ACCEPT
ip6tables -A rn-goodn -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A rn-goodn -j DROP


# Desde la Red Nacional a las computadoras de la red de las sede
ip6tables -A rn-intrn -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A rn-intrn -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A rn-intrn -p tcp ! --syn -j ACCEPT
ip6tables -A rn-intrn -j DROP

# desde la zona desmilitarizada a la universidad dmz-univ
ip6tables -A dmz-univ -j ACCEPT

# desde la universidad a la red de los servidores del nodo univ-goodn

ip6tables -A univ-goodn -s 2001:b00:f80b:200::/64 -j ACCEPT
ip6tables -A univ-goodn -p tcp -s 2001:b00:f80b:3::2/128 -j ACCEPT
ip6tables -A univ-goodn -p tcp -m multiport --dport 22,23,3389 -j DROP
ip6tables -A univ-goodn -p tcp -s 2001:b00:f80b:204::/64 --dport 444 -j
DROP
ip6tables -A univ-goodn -s 2001:b00:f80b:204::2/128 -j ACCEPT
ip6tables -A univ-goodn -s 2001:b00:f80b:204::8/128 -j ACCEPT
ip6tables -A univ-goodn -p tcp \
        -m multiport --dport smtp,pop3,imap,imap3,http,https,ftp,ftp-
data,domain -j ACCEPT
ip6tables -A univ-goodn -p udp -d 2001:b00:f80b:1::3/128  --dport domain
-j ACCEPT
ip6tables -A univ-goodn -p icmpv6 -j icmp-acc
#ip6tables -A univ-goodn -j LOG --log-prefix "univ-goodn"
ip6tables -A univ-goodn -j DROP

# desde la universidad a la red corporativa del nodo univ-intrn
ip6tables -A univ-intrn -s 2001:b00:f80b:3::2/128 -j ACCEPT
ip6tables -A univ-intrn -s 2001:b00:f80b:204::2/128 -j ACCEPT
ip6tables -A univ-intrn -s 2001:b00:f80b:204::8/128 -j ACCEPT
ip6tables -A univ-intrn -s 2001:b00:f80b:200::/64 -j ACCEPT
ip6tables -A univ-intrn -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A univ-intrn -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A univ-intrn -j LOG --log-prefix "univ-intrn"
ip6tables -A univ-intrn -j DROP

# desde la red de los servidores del nodo a la universidad goodn-univ
ip6tables -A goodn-univ -j ACCEPT

# desde la red corporativa del nodo a la universidad intrn-univ
ip6tables -A intrn-univ -p tcp -m multiport --dport 22,23,3389 -j DROP
ip6tables -A intrn-univ -p tcp -d 2001:b00:f80b:200::/64 \
        -m multiport --dport
20,21,25,53,80,110,143,366,389,443,465,563,993,995 -j ACCEPT
ip6tables -A intrn-univ -p udp -d 2001:b00:f80b:200::/64 --dport 53 -j
ACCEPT
ip6tables -A intrn-univ -p tcp -d 2001:b00:f80b:204::/64 -j ACCEPT
ip6tables -A intrn-univ -p udp -d 2001:b00:f80b:200::/64 --dport 53 -j
ACCEPT
```

```
#ip6tables -A intrn-univ -j LOG --log-prefix "intrn-univ "
ip6tables -A intrn-univ -j DROP

# desde la red de los servidores del nodo a la internet goodn-bad
ip6tables -A goodn-bad -p icmpv6 --icmpv6-type ping -j ACCEPT
ip6tables -A goodn-bad -j ACCEPT
#ip6tables -A goodn-bad -j REJECT

# desde la red corporativa del nodo a la internet intrn-bad
#ip6tables -A intrn-bad -j LOG --log-prefix "intrn-bad "

ip6tables -A intrn-bad -j DROP

# desde la universidad a la internet univ-bad
ip6tables -A univ-bad -s 2001:b00:f80b:200::/64 -j ACCEPT
ip6tables -A univ-bad -s 2001:b00:f80b:204::2/128 -j ACCEPT
ip6tables -A univ-bad -s 2001:b00:f80b:204::8/128 -j ACCEPT
ip6tables -A univ-bad -s 2001:b00:f80b:204::10/128 -j ACCEPT
ip6tables -A univ-bad -s 2001:b00:f80b:3::2/128 -j ACCEPT
#ip6tables -A univ-bad -p icmpv6 --icmpv6-type ping -j ACCEPT
#ip6tables -A univ-bad -j LOG --log-prefix "univ-bad "
ip6tables -A univ-bad -j DROP

# desde la internet a la red de los servidores del nodo bayamo

ip6tables -A bad-goodn -d 2001:470:1f07:239::2/128 -p tcp -m multiport \
    --dport ftp,http,https,smtp,pop3,imap,imap3 -j ACCEPT
ip6tables -A bad-goodn -d 2001:470:1f07:239::3/128 -p tcp -m multiport \
    --dport domain,ntp -j ACCEPT
ip6tables -A bad-goodn -d 2001:470:1f07:239::3/128 -p udp -m multiport \
    --dport domain,ntp -j ACCEPT
ip6tables -A bad-goodn -p icmpv6 -j ACCEPT
#ip6tables -A bad-goodn -j LOG --log-prefix "bad-goodn "
ip6tables -A bad-goodn -j ACCEPT

# desde la internet a la red corporativa del nodo bad-intrn
ip6tables -A bad-intrn -j DROP

# desde la internet a la universidad univ-bad
ip6tables -A bad-univ -j DROP

# desde la red de los servidores del nodo a la red corporativa del nodo
ip6tables -A goodn-intrn -j ACCEPT

# desde la red corporativa del nodo a la red de los servidores del nodo
ip6tables -A intrn-goodn -p tcp --dport 3389 -j DROP
ip6tables -A intrn-goodn -p tcp --dport 22 -j DROP
ip6tables -A intrn-goodn -p tcp --dport 23 -j DROP
ip6tables -A intrn-goodn -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A intrn-goodn -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A intrn-goodn -p tcp \
        -m multiport --dport 7,9,11,13,17,19,20,21,25,37 -j ACCEPT
ip6tables -A intrn-goodn -p tcp \
        -m multiport --dport 42,43,53,80,88,101,102,110 -j ACCEPT
ip6tables -A intrn-goodn -p tcp \
        -m multiport --dport 111,113,119,135,137,139,143,158,170,179,194
-j ACCEPT
ip6tables -A intrn-goodn -p tcp \
```

```
        -m multiport --dport
389,366,443,445,464,465,512,513,514,515,520,526,530,531,532 -j ACCEPT
ip6tables -A intrn-goodn -p tcp \
        -m multiport --dport
543,544,556,636,749,993,995,1109,1433,1434,1512 -j ACCEPT
ip6tables -A intrn-goodn -p tcp \
        -m multiport --dport 1524,1723,2053,2967,5001,6112,9535 -j ACCEPT
ip6tables -A intrn-goodn -p tcp -d 2001:b00:f80b:200::/64 --sport 2967 -j
ACCEPT
ip6tables -A intrn-goodn -p tcp \
        -m multiport --dport 15,38,49,106,123,153,160,194,201,202,203 -j
ACCEPT
ip6tables -A intrn-goodn -p tcp \
        -m multiport --dport 204,205,206,207,208,442,593,1026,1029 -j
ACCEPT
ip6tables -A intrn-goodn -p tcp \
        -m multiport --dport 1080,1680,1167,2049,2301,3372 -j ACCEPT
ip6tables -A intrn-goodn -p tcp \
        -m multiport --dport 5631,5632,6112,7070,8010,1521,1720 -j ACCEPT

# UDP
ip6tables -A intrn-goodn -p udp \
        -m multiport --dport 7,9,13,17,19,37,39,42,53,67,68,69,88,111,123
-j ACCEPT
ip6tables -A intrn-goodn -p udp \
        -m multiport --dport 135,137,138,161,162,213 -j ACCEPT
ip6tables -A intrn-goodn -p udp \
        -m multiport --dport 443,445,464,500,512,513 -j ACCEPT
ip6tables -A intrn-goodn -p udp \
        -m multiport --dport
514,517,518,520,525,533,550,560,561,749,1167,1433 -j ACCEPT
ip6tables -A intrn-goodn -p udp \
        -m multiport --dport 1434,1512,1701,1812,1813,2049,5001,6112 -j
ACCEPT
ip6tables -A intrn-goodn -p udp \
        -m multiport --dport 38,49,113,139,153,160,201,202,203 -j ACCEPT
ip6tables -A intrn-goodn -p udp \
        -m multiport --dport 204,205,206,207,208,442,515 -j ACCEPT
ip6tables -A intrn-goodn -p udp \
        -m multiport --dport 750,1028,749,750,1512,1028,2967,6112 -j
ACCEPT
#ip6tables -A intrn-goodn -j LOG --log-prefix "intrn-goodn "
#ip6tables -A intrn-goodn -j ACCEPT
ip6tables -A intrn-goodn -j DROP

ip6tables -N intrn-if
ip6tables -N bad-if
ip6tables -N sit-if
ip6tables -N sum-if
ip6tables -N rn-if
ip6tables -N goodn-if
ip6tables -N dmz-if
ip6tables -N pppn-if
ip6tables -N univ-if

ip6tables -A INPUT -s ::1 -j ACCEPT
ip6tables -A INPUT -s 2001:b00:f80b:3::2 -j ACCEPT
ip6tables -A INPUT -s 2001:b00:ffff:1::2 -j ACCEPT
```

```
ip6tables -A INPUT -i sit1 -j univ-if
ip6tables -A INPUT -i eth0 -j goodn-if
ip6tables -A INPUT -i eth3 -j intrn-if
ip6tables -A INPUT -i eth1 -s 2001:b00:f80b:400::/56 -j sum-if
ip6tables -A INPUT -i eth1 -s 2001:b00:f80b::/64 -j dmz-if
ip6tables -A INPUT -i eth1 -s 2001:b00:f800::/44 -j rn-if
ip6tables -A INPUT -i eth1 -j bad-if
ip6tables -A INPUT -p icmpv6 -j ACCEPT
ip6tables -A INPUT -j DROP

ip6tables -A goodn-if -j ACCEPT

ip6tables -A dmz-if -s 2001:b00:f80b::1/128 -j ACCEPT
ip6tables -A dmz-if -s 2001:b00:f80b::2/128 -j ACCEPT
ip6tables -A dmz-if -s 2001:b00:f80b::4/128 -j ACCEPT
ip6tables -A dmz-if -p icmpv6 -j ACCEPT
ip6tables -A dmz-if -j DROP

ip6tables -A bad-if -s 2001:470:1f07:239::1/128 -j ACCEPT
ip6tables -A bad-if -p tcp --dport 80 -j ACCEPT
ip6tables -A bad-if -p tcp --dport 20 -j ACCEPT
ip6tables -A bad-if -p tcp --dport 21 -j ACCEPT
ip6tables -A bad-if -p tcp --dport 995 -j ACCEPT
ip6tables -A bad-if -p tcp --dport 443 -j ACCEPT
ip6tables -A bad-if -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A bad-if -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A bad-if -p icmpv6 -j ACCEPT
#ip6tables -A bad-if -j LOG --log-prefix "bad-if "
ip6tables -A bad-if -j DROP

ip6tables -A rn-if -p tcp --dport 80 -j ACCEPT
ip6tables -A rn-if -p tcp --dport 20 -j ACCEPT
ip6tables -A rn-if -p tcp --dport 21 -j ACCEPT
ip6tables -A rn-if -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A rn-if -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A rn-if -p icmpv6 -j ACCEPT

#ip6tables -A rn-if -j LOG --log-prefix "rn-if "
ip6tables -A rn-if -j DROP

ip6tables -A sum-if -p tcp --dport 80 -j ACCEPT
ip6tables -A sum-if -p tcp --dport 20 -j ACCEPT
ip6tables -A sum-if -p tcp --dport 21 -j ACCEPT
ip6tables -A sum-if -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A sum-if -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A sum-if -p icmpv6 -j ACCEPT
#ip6tables -A sum-if -j LOG --log-prefix "sum-if "
ip6tables -A sum-if -j DROP

ip6tables -A univ-if -s 2001:b00:f80b:204::2/128 -j ACCEPT
ip6tables -A univ-if -s fe80::c0a8:fb02/128 -j ACCEPT
ip6tables -A univ-if -s fe00::/8 -j ACCEPT
ip6tables -A univ-if -s 2001:b00:f80b:204::1/128 -j ACCEPT
ip6tables -A univ-if -s 2001:b00:f80b:3::2/128 -j ACCEPT
ip6tables -A univ-if -s 2001:b00:f80b:200::/64 -j ACCEPT
ip6tables -A univ-if -p tcp --dport 20 -j ACCEPT
ip6tables -A univ-if -p tcp --dport 21 -j ACCEPT
ip6tables -A univ-if -p tcp --dport 80 -j ACCEPT
```

```
ip6tables -A univ-if -p icmpv6 -j ACCEPT
#ip6tables -A univ-if -j LOG --log-prefix "univ-if "
ip6tables -A univ-if -j DROP

ip6tables -A intrn-if -p tcp --dport 80 -j ACCEPT
ip6tables -A intrn-if -p tcp --dport 20 -j ACCEPT
ip6tables -A intrn-if -p tcp --dport 21 -j ACCEPT
ip6tables -A intrn-if -p tcp --sport 53 -j ACCEPT
ip6tables -A intrn-if -p udp --sport 53 -j ACCEPT
#ip6tables -A intrn-if -p udp --sport 67 -j ACCEPT
#ip6tables -A intrn-if -p udp --sport 68 -j ACCEPT
#ip6tables -A intrn-if -p udp --dport 67 -j ACCEPT
#ip6tables -A intrn-if -p udp --dport 68 -j ACCEPT
ip6tables -A intrn-if -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A intrn-if -p icmpv6 -j ACCEPT
#ip6tables -A intrn-if -j LOG --log-prefix "intr-if "
ip6tables -A intrn-if -j DROP

ip6tables -D INPUT 1
ip6tables -D FORWARD 1
ip6tables -D OUTPUT 1
```

Anexo 6B. Script para la creación de las reglas de los cortafuegos en IP6Tables en el router elektra.udg.co.cu (Archivo /iptables/ip6tables)

```
ip6tables -F INPUT
ip6tables -F FORWARD
ip6tables -F OUTPUT

ip6tables -A INPUT -j DROP
ip6tables -A FORWARD -j DROP
ip6tables -A OUTPUT -j DROP

ip6tables -N good-dmz
ip6tables -N eco-dmz
ip6tables -N coor-dmz
ip6tables -N coor-goodn
ip6tables -N dmz-good
ip6tables -N dmz-eco
ip6tables -N dmz-coor

ip6tables -N good-goodn
ip6tables -N eco-goodn
ip6tables -N goodn-good
ip6tables -N goodn-eco
ip6tables -N goodn-coor

ip6tables -N good-intrn
ip6tables -N eco-intrn
ip6tables -N coor-intrn
ip6tables -N intrn-good
ip6tables -N intrn-eco
ip6tables -N intrn-coor

ip6tables -N good-fir
ip6tables -N eco-fir
```

```
ip6tables -N coor-fir
ip6tables -N fir-good
ip6tables -N fir-eco
ip6tables -N fir-coor

ip6tables -N good-bad
ip6tables -N bad-good
ip6tables -N good-eco
ip6tables -N eco-good
ip6tables -N good-coor
ip6tables -N coor-good
ip6tables -N bad-eco
ip6tables -N eco-bad
ip6tables -N bad-coor
ip6tables -N coor-bad

ip6tables -N eco-coor
ip6tables -N coor-eco
ip6tables -N icmp-acc

ip6tables -A FORWARD -m state --state INVALID -j DROP
ip6tables -A FORWARD -m state --state RELATED,ESTABLISHED -j ACCEPT

###############
# Chains Jump #
###############

ip6tables -A FORWARD -s 2001:b00:f80b:200::/64 -d 2001:b00:f80b:3::1/128
-o sit1 -j good-fir
ip6tables -A FORWARD -s 2001:b00:f80b:200::/64 -d 2001:470:1f07:239::/64
-o sit1 -j good-goodn
ip6tables -A FORWARD -s 2001:b00:f80b:200::/64 -d 2001:b00:f80b::/64 -o
sit1 -j good-dmz
ip6tables -A FORWARD -s 2001:b00:f80b:200::/64 -d 2001:b00:f80b:4::/64 -o
sit1 -j good-intrn
ip6tables -A FORWARD -s 2001:b00:f80b:200::/64 -d 2001:b00:f80b:204::/64
-o eth3 -j good-coor
ip6tables -A FORWARD -s 2001:b00:f80b:200::/64 -d 2001:b00:f80b:208::/64
-o eth2 -j good-eco
ip6tables -A FORWARD -s 2001:b00:f80b:208::/64 -d 2001:b00:f80b:3::1/128
-o sit1 -j eco-fir
ip6tables -A FORWARD -s 2001:b00:f80b:208::/64 -d 2001:b00:f80b::/64 -o
sit1 -j eco-dmz
ip6tables -A FORWARD -s 2001:b00:f80b:208::/64 -d 2001:470:1f07:239::/64
-o sit1 -j eco-goodn
ip6tables -A FORWARD -s 2001:b00:f80b:208::/64 -d 2001:b00:f80b:4::/64 -o
sit1 -j eco-intrn
ip6tables -A FORWARD -s 2001:b00:f80b:208::/64 -d 2001:b00:f80b:204::/64
-o eth3 -j eco-coor
ip6tables -A FORWARD -s 2001:b00:f80b:208::/64 -d 2001:b00:f80b:200::/64
-o eth0 -j eco-good
ip6tables -A FORWARD -s 2001:b00:f80b:204::/64 -d 2001:b00:f80b:3::1/128
-o sit1 -j coor-fir
ip6tables -A FORWARD -s 2001:b00:f80b:204::/64 -d 2001:b00:f80b::/64 -o
sit1 -j coor-dmz
ip6tables -A FORWARD -s 2001:b00:f80b:204::/64 -d 2001:470:1f07:239::/64
-o sit1 -j coor-goodn
```

```
ip6tables -A FORWARD -s 2001:b00:f80b:204::/64 -d 2001:b00:f80b:4::/64 -o
sit1 -j coor-intrn
ip6tables -A FORWARD -s 2001:b00:f80b:204::/64 -d 2001:b00:f80b:200::/64
-o eth0 -j coor-good
ip6tables -A FORWARD -s 2001:b00:f80b:204::/64 -d 2001:b00:f80b:208::/64
-o eth2 -j coor-eco
ip6tables -A FORWARD -s 2001:b00:f80b::/64 -d 2001:b00:f80b:200::/64 -o
eth0 -j dmz-good
ip6tables -A FORWARD -s 2001:b00:f80b::/64 -d 2001:b00:f80b:208::/64 -o
eth2 -j dmz-eco
ip6tables -A FORWARD -s 2001:b00:f80b::/64 -d 2001:b00:f80b:204::/64 -o
eth3 -j dmz-coor
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -d 2001:b00:f80b:208::/64 -o
eth2 -j intrn-eco
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -d 2001:b00:f80b:204::/64 -o
eth3 -j intrn-coor
ip6tables -A FORWARD -s 2001:b00:f80b:4::/64 -d 2001:b00:f80b:200::/64 -o
eth0 -j intrn-good
ip6tables -A FORWARD -s 2001:b00:f80b:3::1/128 -d 2001:b00:f80b:200::/64
-o eth0 -j fir-good
ip6tables -A FORWARD -s 2001:b00:f80b:3::1/128 -d 2001:b00:f80b:208::/64
-o eth2 -j fir-eco
ip6tables -A FORWARD -s 2001:b00:f80b:3::1/128 -d 2001:b00:f80b:204::/64
-o eth3 -j fir-coor
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -d 2001:b00:f80b:200::/64
-o eth0 -j goodn-good
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -d 2001:b00:f80b:208::/64
-o eth2 -j goodn-eco
ip6tables -A FORWARD -s 2001:470:1f07:239::/64 -d 2001:b00:f80b:204::/64
-o eth3 -j goodn-coor
ip6tables -A FORWARD -i eth0 -o sit1 -j good-bad
ip6tables -A FORWARD -i eth2 -o sit1 -j eco-bad
ip6tables -A FORWARD -i eth3 -o sit1 -j coor-bad
ip6tables -A FORWARD -o eth0 -j bad-good
ip6tables -A FORWARD -o eth2 -j bad-eco
ip6tables -A FORWARD -o eth3 -j bad-coor
ip6tables -A FORWARD -j DROP

ip6tables -A icmp-acc -p icmpv6 --icmpv6-type echo-request -j ACCEPT
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type ping -j ACCEPT
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type echo-reply -j ACCEPT
ip6tables -A icmp-acc -p icmpv6 --icmpv6-type parameter-problem -j ACCEPT
#ip6tables -A icmp-acc -j LOG --log-prefix "icmpv6-acc "
ip6tables -A icmp-acc -j DROP

#good-goodn
ip6tables -A good-goodn -j ACCEPT

#eco-goodn
ip6tables -A eco-goodn -p tcp \
        -m multiport --dport
20,21,25,80,110,143,366,389,443,465,563,993,995 -j ACCEPT
#ip6tables -A eco-goodn -j LOG --log-prefix "eco-goodn "
ip6tables -A eco-goodn -j DROP

# coor-goodn
ip6tables -A coor-goodn -p tcp \
       -m multiport --dport 22,23,3389 -j DROP
```

```
ip6tables -A coor-goodn -p udp \
       -m multiport --dport 22,23,3389 -j DROP
ip6tables -A coor-goodn -s 2001:b00:f80b:204::2/128 -j ACCEPT
ip6tables -A coor-goodn -s 2001:b00:f80b:204::8/128 -j ACCEPT
ip6tables -A coor-goodn -p tcp \
        -m multiport --dport
20,21,25,80,110,143,366,389,443,465,563,993,995 -j ACCEPT
ip6tables -A coor-goodn -p tcp \
        -m multiport --dport 5222,5223,5228,5269,7301,7302,7303,7304,7334
-j ACCEPT
#ip6tables -A coor-goodn -j LOG --log-prefix "coor-goodn "
ip6tables -A coor-goodn -j DROP

#good-dmz
#ip6tables -A good-dmz -j LOG --log-prefix "good-dmz "
ip6tables -A good-dmz -j ACCEPT

# eco-dmz
ip6tables -A eco-dmz -p tcp \
         -m multiport --dport http,ftp,ftp-data,domain -j ACCEPT
ip6tables -A eco-dmz -p udp --dport domain -j ACCEPT
ip6tables -A eco-dmz -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A eco-dmz -p udp --dport 1024:65535 -j ACCEPT
#ip6tables -A eco-dmz -j LOG --log-prefix "eco-dmz "
ip6tables -A eco-dmz -j DROP

# coor-dmz
ip6tables -A coor-dmz -p tcp \
       -m multiport --dport 22,23,3389 -j DROP
ip6tables -A coor-dmz -s 2001:b00:f80b:204::2/128 -j ACCEPT
ip6tables -A coor-dmz -s 2001:b00:f80b:204::8/128 -j ACCEPT
ip6tables -A coor-dmz -p tcp \
         -m multiport --dport http,ftp,ftp-data -j ACCEPT
ip6tables -A coor-dmz -p udp --dport domain -j ACCEPT
ip6tables -A coor-dmz -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A coor-dmz -p udp --dport 1024:65535 -j ACCEPT
#ip6tables -A coor-dmz -j LOG --log-prefix "coor-dmz "
#ip6tables -A coor-dmz -p icmpv6 -j icmp-acc
ip6tables -A coor-dmz -j DROP

#good-intrn
#ip6tables -A good-intrn -j LOG --log-prefix "good-intrn "
ip6tables -A good-intrn -j ACCEPT

#eco-intrn
#ip6tables -A eco-intrn -j LOG --log-prefix "eco-coor "
ip6tables -A eco-intrn -j ACCEPT

#coor-intrn
ip6tables -A coor-intrn -j ACCEPT

#good-coor
# red de los servidores a la intranet
#ip6tables -A good-coor -j LOG --log-prefix "good-coor "
ip6tables -A good-coor -j ACCEPT

#eco-coor
#ip6tables -A eco-coor -j LOG --log-prefix "eco-coor "
```

```
ip6tables -A eco-coor -j ACCEPT

# coor-good
# desde la intranet a la red de los servidores
ip6tables -A coor-good -p tcp -m multiport --dport 22,23,3389 -j DROP
ip6tables -A coor-good -s 2001:b00:f80b:204::2/128 -j ACCEPT
ip6tables -A coor-good -s 2001:b00:f80b:204::8/128 -j ACCEPT
ip6tables -A coor-good -p tcp -s 2001:b00:f80b:204::13/128 -d
2001:b00:f80b:200::5/128 -m multiport --dport 3306,1433,1434 -j ACCEPT
ip6tables -A coor-good -p udp -s 2001:b00:f80b:204::13/128 -d
2001:b00:f80b:200::5/128 -m multiport --dport 3306,1433,1434 -j ACCEPT
ip6tables -A coor-good -p tcp -s 2001:b00:f80b:204::10/128 -m mac --mac-
source 00:11:11:6f:0e:19 -j ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport 7,9,11,13,17,19,20,21,25,37 -j ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport 42,43,53,80,88,101,102,110 -j ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport 111,113,119,135,137,139,143,158,170,179,194
-j ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport
389,366,443,445,464,465,512,513,514,515,520,526,530,531,532 -j ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport
543,544,556,636,749,993,995,1109,1433,1434,1512 -j ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport 1524,1723,1755,2053,2967,5001,6112,9535 -j
ACCEPT
ip6tables -A coor-good -p tcp --sport 2967 -j ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport 15,38,49,106,123,153,160,194,201,202,203 -j
ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport 204,205,206,207,208,442,593,1026,1029 -j
ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport 1080,1680,1167,2049,2301,3372,8082 -j ACCEPT
ip6tables -A coor-good -p tcp \
        -m multiport --dport 5631,5632,6112,7070,8010,1521,1720 -j ACCEPT

# UDP
ip6tables -A coor-good -p udp \
        -m multiport --dport 7,9,13,17,19,37,39,42,53,67,68,69,88,111,123
-j ACCEPT
ip6tables -A coor-good -p udp \
        -m multiport --dport 135,137,138,161,162,213 -j ACCEPT
ip6tables -A coor-good -p udp \
        -m multiport --dport 443,445,464,500,512,513 -j ACCEPT
ip6tables -A coor-good -p udp \
        -m multiport --dport
514,517,518,520,525,533,550,560,561,749,1167,1433 -j ACCEPT
ip6tables -A coor-good -p udp \
        -m multiport --dport 1434,1512,1701,1755,1812,1813,2049,5001,6112
-j ACCEPT
ip6tables -A coor-good -p udp \
        -m multiport --dport 38,49,113,139,153,160,201,202,203 -j ACCEPT
ip6tables -A coor-good -p udp \
```

```
        -m multiport --dport 204,205,206,207,208,442,515 -j ACCEPT
ip6tables -A coor-good -p udp \
        -m multiport --dport 750,1028,749,750,1512,1028,2967,6112 -j
ACCEPT
# ip6tables -A coor-good -j LOG --log-prefix "coor-good "
# ip6tables -A coor-good -j ACCEPT
ip6tables -A coor-good -j DROP

ip6tables -A good-eco -j ACCEPT

#eco-good
ip6tables -A eco-good -p tcp \
        -m multiport --dport
20,21,25,80,110,143,366,389,443,465,563,993,995 -j ACCEPT
ip6tables -A eco-good -p udp --dport 53 -j ACCEPT
# ip6tables -A eco-good -j LOG --log-prefix "eco-good "
ip6tables -A eco-good -j DROP

#coor-eco
ip6tables -A coor-eco -s 2001:b00:f80b:204::88/128 -d
2001:b00:f80b:208::1e/128 -j ACCEPT
ip6tables -A coor-eco -p tcp ! --syn -s 2001:b00:f80b:204::/64 -j ACCEPT
# ip6tables -A coor-eco -j LOG --log-prefix "coor-eco "
ip6tables -A coor-eco -j DROP

# dmz-good
ip6tables -A dmz-good -p tcp ! --syn -j ACCEPT
ip6tables -A dmz-good -p udp --dport domain -j ACCEPT
ip6tables -A dmz-good -p tcp \
       -m multiport --dport ftp,ftp-
data,https,http,smtp,pop2,pop3,imap,imap3 -j ACCEPT
ip6tables -A dmz-good -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A dmz-good -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A dmz-good -p icmpv6 -j icmp-acc
ip6tables -A dmz-good -j DROP

# dmz-eco
ip6tables -A dmz-eco -p tcp ! --syn -j ACCEPT
ip6tables -A dmz-eco -p udp --dport domain -j ACCEPT
#ip6tables -A dmz-eco -j LOG --log-prefix "dmz-eco "
ip6tables -A dmz-eco -p icmpv6 -j icmp-acc
ip6tables -A dmz-eco -j DROP

#dmz-coor
ip6tables -A dmz-coor -p tcp ! --syn --sport ftp -j ACCEPT
ip6tables -A dmz-coor -p tcp ! --syn --sport ftp-data -j ACCEPT
ip6tables -A dmz-coor -p tcp ! --syn --sport http -j ACCEPT
ip6tables -A dmz-coor -p tcp ! --syn --sport https -j ACCEPT
ip6tables -A dmz-coor -p tcp ! --syn --sport domain -j ACCEPT
ip6tables -A dmz-coor -p udp --dport domain -j ACCEPT
ip6tables -A dmz-coor -p tcp ! --syn --sport 1024:65535 -j ACCEPT
ip6tables -A dmz-coor -p udp --dport 1024:65535 -j ACCEPT
ip6tables -A dmz-coor -p tcp \
        -m multiport --dport http,https,ftp,ftp-data -j ACCEPT
#ip6tables -A dmz-coor -j LOG --log-prefix "dmz-coor "
ip6tables -A dmz-coor -p icmpv6 -j icmp-acc
ip6tables -A dmz-coor -j DROP
```

```
#intrn-eco
#ip6tables -A intrn-eco -j LOG --log-prefix "intrn-eco "
ip6tables -A intrn-eco -j DROP

#ip6tables -A intrn-coor -j LOG --log-prefix "intrn-coor "
ip6tables -A intrn-coor -j ACCEPT

#intrn-good
ip6tables -A intrn-good -p tcp \
        -m multiport --dport
20,21,25,80,110,143,366,389,443,465,563,993,995 -j ACCEPT
#ip6tables -A intrn-good -j LOG --log-prefix "intrn-good "
ip6tables -A intrn-good -j DROP

#goodn-good
ip6tables -A goodn-good -j ACCEPT

#goodn-eco
ip6tables -A goodn-eco -j ACCEPT

#goodn-coor
ip6tables -A goodn-coor -j ACCEPT

# desde la red de los servidores a la internet
ip6tables -A good-bad -j ACCEPT

#eco-bad
#ip6tables -A eco-bad -j LOG --log-prefix "eco-bad "
ip6tables -A eco-bad -j DROP

#coor-bad
ip6tables -A coor-bad -s 2001:b00:f80b:204::2/128 -m mac --mac-source
00:B0:D0:AA:EC:58 -j ACCEPT
ip6tables -A coor-bad -s 2001:b00:f80b:204::8/128 -m mac --mac-source
00:40:F4:71:77:6E -j ACCEPT
ip6tables -A coor-bad -s 2001:b00:f80b:204::10/128 -m mac --mac-source
00:11:11:6F:0E:19 -j ACCEPT
ip6tables -A coor-bad -p icmpv6 -j icmp-acc
ip6tables  -A coor-bad -d 2001:b00:f800::/44 -j ACCEPT
#ip6tables -A coor-bad -j LOG --log-prefix "coor-bad "
ip6tables -A coor-bad -j DROP

#bad-good
ip6tables -A bad-good -p tcp -s 2001:b00:f800::/44 \
     -m multiport --dport domain,smtp,pop3,imap,imap3,http,https,ftp,ftp-
data,ntp,domain -j ACCEPT
ip6tables -A bad-good -s 2001:b00:f800::/44 -p tcp --dport 1024:65535 -j
ACCEPT
ip6tables -A bad-good -p udp -s 2001:b00:f800::/44 \
     -m multiport --dport ntp,domain -j ACCEPT
ip6tables -A bad-good -s 2001:b00:f800::/44 -p udp --dport 1024:65535 -j
ACCEPT
ip6tables -A bad-good -p icmpv6 -s 2001:b00:f800::/44 -j icmp-acc
ip6tables -A bad-good -j DROP

#bad-eco
#ip6tables -A bad-eco -j LOG --log-prefix "bad-eco "
ip6tables -A bad-eco -j DROP
```

```
#
# bad-coor
ip6tables -A bad-coor -s 2001:b00:f800::/44 -j ACCEPT

ip6tables -A bad-coor -s 2001:b00:f800::/44 -p tcp \
         -m multiport --dport smtp,pop3,imap,imap3,http,https,ftp,ftp-
data,domain -j ACCEPT
ip6tables -A bad-coor -s 2001:b00:f800::/44 -p udp --dport domain -j
ACCEPT
ip6tables -A bad-coor -s 2001:b00:f800::/44 -p tcp --dport 1024:65535 -j
ACCEPT
ip6tables -A bad-coor -s 2001:b00:f800::/44 -p udp --dport 1024:65535 -j
ACCEPT
ip6tables -A bad-coor -p icmpv6 -j icmp-acc
ip6tables -A bad-coor -j DROP

#good-fir
ip6tables -A good-fir -j ACCEPT

#eco-fir
ip6tables -A eco-fir -p tcp \
         -m multiport --dport ftp,ftp-data,http,https -j ACCEPT
ip6tables -A eco-fir -p tcp --dport 3132 -j ACCEPT
#ip6tables -A eco-fir -j LOG --log-prefix "eco-fir "
ip6tables -A eco-fir -j DROP

#coor-fir
ip6tables -A coor-fir -s 2001:b00:f80b:204::2/128 -j ACCEPT
ip6tables -A coor-fir -p tcp \
         -m multiport --dport ftp,ftp-data,http,https -j ACCEPT
ip6tables -A coor-fir -p tcp --dport 3132 -j ACCEPT
ip6tables -A coor-fir -p tcp --dport 5222 -j ACCEPT
ip6tables -A coor-fir -p udp --dport 5222 -j ACCEPT
#ip6tables -A coor-fir -p tcp --dport 1024:65535 -j ACCEPT
#ip6tables -A coor-fir -p udp --dport 1024:65535 -j ACCEPT
#ip6tables -A coor-fir -j LOG --log-prefix "coor-fir "
ip6tables -A coor-fir -j DROP

#fir-good
ip6tables -A fir-good -j ACCEPT

#fir-eco
ip6tables -A fir-eco -j ACCEPT

#fir-coor
ip6tables -A fir-coor -j ACCEPT

# Nodo Bayamo: 2001:b00:f80b::/56
# SUMs: 2001:b00:f80b:400::/56
# Universidad: 2001:b00:f80b:200/56

ip6tables -N intr-if
ip6tables -N bad-if
ip6tables -N good-if
ip6tables -N eco-if
ip6tables -N dmz-if
ip6tables -N goodn-if
ip6tables -N sum-if
```

```
ip6tables -N rn-if

ip6tables -A INPUT -i sit1 -s fe80::c0a8:fa02/128 -j ACCEPT
ip6tables -A INPUT -i sit1 -s ff00::/8 -j ACCEPT
ip6tables -A INPUT -i sit1 -s 2001:b00:f80b::/64 -j dmz-if
ip6tables -A INPUT -i sit1 -s 2001:470:1f07:239::/64 -j goodn-if
ip6tables -A INPUT -i sit1 -s 2001:b00:f80b:400::/54 -j sum-if
ip6tables -A INPUT -i sit1 -s 2001:b00:f800::/44 -j rn-if
ip6tables -A INPUT -i sit1 -j bad-if
ip6tables -A INPUT -i eth0 -j good-if
ip6tables -A INPUT -i eth2 -j eco-if
ip6tables -A INPUT -i eth3 -j intr-if
ip6tables -A INPUT -j DROP

ip6tables -A dmz-if -s 2001:b00:f80b::1/128 -j ACCEPT
ip6tables -A dmz-if -s 2001:b00:f80b::2/128 -j ACCEPT
ip6tables -A dmz-if -s 2001:b00:f80b::3/128 -j ACCEPT
ip6tables -A dmz-if -s 2001:b00:f80b::4/128 -j ACCEPT

ip6tables -A goodn-if -j ACCEPT

ip6tables -A good-if -j ACCEPT

ip6tables -A eco-if -p tcp --dport 80 -j ACCEPT
ip6tables -A eco-if -p tcp --dport 20 -j ACCEPT
ip6tables -A eco-if -p tcp --dport 21 -j ACCEPT
ip6tables -A eco-if -p tcp --sport 53 -j ACCEPT
ip6tables -A eco-if -p udp --sport 53 -j ACCEPT
ip6tables -A eco-if -p tcp --dport 1024:65535 -j ACCEPT
####ip6tables -A eco-if -p icmpv6 -j icmp-acc
ip6tables -A eco-if -p icmpv6 -j ACCEPT
#ip6tables -A eco-if -j LOG --log-prefix "eco-if "
ip6tables -A eco-if -j DROP

ip6tables -A sum-if -p tcp --dport 80 -j ACCEPT
ip6tables -A sum-if -p tcp --dport 20 -j ACCEPT
ip6tables -A sum-if -p tcp --dport 21 -j ACCEPT
ip6tables -A sum-if -p tcp --sport 53 -j ACCEPT
ip6tables -A sum-if -p udp --sport 53 -j ACCEPT
ip6tables -A sum-if -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A sum-if -p icmpv6 -j ACCEPT
#ip6tables -A sum-if -j LOG --log-prefix "sum-if "
ip6tables -A sum-if -j DROP

ip6tables -A rn-if -p tcp --dport 80 -j ACCEPT
ip6tables -A rn-if -p tcp --dport 20 -j ACCEPT
ip6tables -A rn-if -p tcp --dport 21 -j ACCEPT
ip6tables -A rn-if -p tcp --sport 53 -j ACCEPT
ip6tables -A rn-if -p udp --sport 53 -j ACCEPT
ip6tables -A rn-if -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A rn-if -p icmpv6 -j ACCEPT
#ip6tables -A rn-if -j LOG --log-prefix "rn-if "
ip6tables -A rn-if -j DROP

ip6tables -A bad-if -s 2001:b00:f80b:3::1/128 -j ACCEPT
ip6tables -A bad-if -p tcp --dport 80 -j ACCEPT
ip6tables -A bad-if -p tcp --dport 20 -j ACCEPT
ip6tables -A bad-if -p tcp --dport 21 -j ACCEPT
```

```
ip6tables -A bad-if -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A bad-if -p icmpv6 -j ACCEPT
#ip6tables -A bad-if -j LOG --log-prefix "bad-if "
ip6tables -A bad-if -j DROP

ip6tables -A intr-if -p tcp --dport 80 -j ACCEPT
ip6tables -A intr-if -p tcp --dport 20 -j ACCEPT
ip6tables -A intr-if -p tcp --dport 21 -j ACCEPT
ip6tables -A intr-if -p tcp --sport 53 -j ACCEPT
ip6tables -A intr-if -p udp --sport 53 -j ACCEPT
ip6tables -A intr-if -p tcp --dport 1024:65535 -j ACCEPT
ip6tables -A intr-if -p icmpv6 -j ACCEPT
#ip6tables -A intr-if -j LOG --log-prefix "intr-if "
ip6tables -A intr-if -j DROP

ip6tables -D INPUT 1
ip6tables -D FORWARD 1
ip6tables -D OUTPUT 1
```

Anexo 7A. Configuración del servicio "Router Advertisement" en el servidor antares.udg.co.cu. (Archivo /etc/radvd.conf)

```
interface eth0
# Enviara "mensajes de anuncios" en la red de la interfase
# eth0 (Red Interna de los servidores del nodo central de
# Bayamo.
{
               AdvSendAdvert on;
               prefix 2001:470:1f07:239::/64

# Prefijo a indicar a los clientes en el mensaje de anuncio

               {
                   AdvOnLink on;

# Indica que este prefijo puede ser usado para detecciones
# on-link. Cuando no se activa, la advertencia se hace sin
# estado de enlace del prefijo.

                   AdvAutonomous on;

# Indica que el prefijo puede utilizarce para la
# configuracion automatica de las direcciones segun el
# RFC 2462.
               };
};
interface eth3
{
               AdvSendAdvert on;
               prefix 2001:b00:f80b:4::/64
               {
                   AdvOnLink on;
                   AdvAutonomous on;
               };
};
```

Anexo 7B. Configuración del servicio "Router Advertisement" en el servidor elektra.udg.co.cu. (Archivo /etc/radvd.conf)

```
interface eth3
{
        AdvSendAdvert on;
                prefix 2001:b00:f80b:204::/64
                {
                    AdvOnLink on;
                    AdvAutonomous on;
                };
};
interface eth0
{
        AdvSendAdvert on;
                prefix 2001:b00:f80b:200::/64
                {
                    AdvOnLink on;
                    AdvAutonomous on;
                };
};
interface eth2
{
        AdvSendAdvert on;
                prefix 2001:b00:f80b:208::/64
                {
                    AdvOnLink on;
                    AdvAutonomous on;
                };
};
```

Anexo 8A. Declaración de las zonas externas en el DNS oficial de la Universidad de Granma. (Archivo /var/named/chroot/etc/named.rfc1912.external.zones)

```
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
//
// See /usr/share/doc/bind*/sample/ for example named configuration
files.
//
zone "." IN {
        type hint;
        file "named.ca";
```

```
};

zone "localdomain" IN {
        type master;
        file "localdomain.zone";
        allow-update { none; };
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
};


zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
};

zone "0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa" IN {
         type master;
        file "named.ip6.local";
        allow-update { none; };
};

zone "255.in-addr.arpa" IN {
        type master;
        file "named.broadcast";
        allow-update { none; };
};

zone "0.in-addr.arpa" IN {
        type master;
        file "named.zero";
        allow-update { none; };
};

zone "udg.co.cu" IN {
        type master;
        file "data/udg.co.cu";
        allow-update { none; };
};

zone  "8/29.149.55.200.in-addr.arpa" IN {
        type master;
        file "data/149.55.200.in-addr.arpa";
        allow-update { none; };
};


zone  "0/27.53.14.200.in-addr.arpa" IN {
        type master;
        file "data/53.14.200.in-addr.arpa";
        allow-update { none; };
};
```

Anexo 8B. Declaración de las zonas internas en el DNS oficial de la Universidad de Granma. (Archivo /var/named/chroot/etc/named.rfc1912.internal.zones)

```
// named.rfc1912.zones:
//
// Provided by Red Hat caching-nameserver package
//
// ISC BIND named zone configuration for zones recommended by
// RFC 1912 section 4.1 : localhost TLDs and address zones
//
// See /usr/share/doc/bind*/sample/ for example named configuration
files.
//

zone "." IN {
        type hint;
        file "named.ca";
};

zone "localhost" IN {
        type master;
        file "localhost.zone";
        allow-update { none; };
        allow-transfer { none; };
};

zone "0.0.127.in-addr.arpa" IN {
        type master;
        file "named.local";
        allow-update { none; };
        allow-transfer { none; };
};

zone  "1.24.10.in-addr.arpa" IN {
        type master;
        file  "data/internal/1.24.10.in-addr.arpa";
        allow-update { none; };
};

zone  "6.24.10.in-addr.arpa" IN {
        type master;
        file  "data/internal/6.24.10.in-addr.arpa";
        allow-update { none; };
};

zone  "7.24.10.in-addr.arpa" IN {
        type master;
        file  "data/internal/7.24.10.in-addr.arpa";
        allow-update { none; };
};


zone  "100.24.10.in-addr.arpa" IN {
        type master;
        file  "data/internal/100.24.10.in-addr.arpa";
        allow-update { none; };
};
```

```
// Rio Cauto
zone  "0.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/0.25.10.in-addr.arpa";
        allow-update { none; };
};

// Cauto Cristo
zone  "2.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/2.25.10.in-addr.arpa";
        allow-update { none; };
};

// Jiguani
zone  "4.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/4.25.10.in-addr.arpa";
        allow-update { none; };
};

// Bayamo
zone  "6.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/6.25.10.in-addr.arpa";
        allow-update { none; };
};

// Yara
zone  "8.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/8.25.10.in-addr.arpa";
        allow-update { none; };
};

// Manzanillo
zone  "10.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/10.25.10.in-addr.arpa";
        allow-update { none; };
};

// Campechuela
zone  "12.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/12.25.10.in-addr.arpa";
        allow-update { none; };
};

// Media Luna
zone  "14.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/14.25.10.in-addr.arpa";
        allow-update { none; };
};

// Niquero
zone  "16.25.10.in-addr.arpa" IN {
```

```
        type master;
        file "data/internal/16.25.10.in-addr.arpa";
        allow-update { none; };
};

// Pilon
zone  "18.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/18.25.10.in-addr.arpa";
        allow-update { none; };
};

// Bartolome Maso
zone  "20.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/20.25.10.in-addr.arpa";
        allow-update { none; };
};

// Buey Arriba
zone  "22.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/22.25.10.in-addr.arpa";
        allow-update { none; };
};

// Guisa
zone  "24.25.10.in-addr.arpa" IN {
        type master;
        file "data/internal/24.25.10.in-addr.arpa";
        allow-update { none; };
};

zone  "251.168.192.in-addr.arpa" IN {
        type master;
        file  "data/internal/251.168.192.in-addr.arpa";
        allow-update { none; };
};

zone  "254.168.192.in-addr.arpa" IN {
        type master;
        file  "data/internal/254.168.192.in-addr.arpa";
        allow-update { none; };
};

zone  "8/29.149.55.200.in-addr.arpa" IN {
        type master;
        file "data/internal/149.55.200.in-addr.arpa";
        allow-update { none; };
};

zone  "0/27.53.14.200.in-addr.arpa" IN {
        type master;
        file "data/internal/53.14.200.in-addr.arpa";
        allow-update { none; };
};

zone  "4.168.192.in-addr.arpa" IN {
```

```
        type master;
        file  "data/internal/4.168.192.in-addr.arpa";
        allow-update { none; };
};

zone  "0.168.192.in-addr.arp" IN {
        type master;
        file  "data/internal/0.168.192.in-addr.arpa";
        allow-update { none; };
};

zone "udg.co.cu" IN {
        type master;
        file "data/internal/udg.co.cu";
        allow-query { any; };
        allow-update { 200.14.53.0/27; 10.24.1.0/24; 10.24.6.2; 10.24.6.8;
};
//      allow-update { none; };
};

zone "0.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa" IN {
        type master;
        file
"data/internal/ipv6rev/0.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa";
        allow-update { none; };
};

zone "8.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa" IN {
        type master;
        file
"data/internal/ipv6rev/8.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa";
        allow-update { none; };
};
zone "9.3.2.0.7.0.f.1.0.7.4.0.1.0.0.2.ip6.arpa" IN {
        type master;
        file
"data/internal/ipv6rev/9.3.2.0.7.0.f.1.0.7.4.0.1.0.0.2.ip6.arpa";
        allow-update { none; };
};
zone "9.3.2.0.6.0.f.1.0.7.4.0.1.0.0.2.ip6.arpa" IN {
        type master;
        file
"data/internal/ipv6rev/9.3.2.0.6.0.f.1.0.7.4.0.1.0.0.2.ip6.arpa";
        allow-update { none; };
};
zone "3.0.0.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa" IN {
        type master;
        file
"data/internal/ipv6rev/3.0.0.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa";
        allow-update { none; };
};

zone "4.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa" IN {
        type master;
        file
"data/internal/ipv6rev/4.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa";
        allow-update { none; };
};
```

```
zone "0.0.0.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa" IN {
        type master;
        file
"data/internal/ipv6rev/0.0.0.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa";
        allow-update { none; };
};

zone "4.0.0.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa" IN {
        type master;
        file
"data/internal/ipv6rev/4.0.0.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa";
        allow-update { none; };
};

zone "reduc.edu.cu" {
        type slave;
        masters { 200.55.147.2; };
        file "slaves/reduc.edu.cu";
};

zone "unica.cu" {
        type slave;
        masters { 200.55.147.66; };
        file "slaves/unica.cu";
};

zone "cug.co.cu" {
        type slave;
        masters { 200.55.149.142; };
        file "slaves/cug.co.cu";
};

zone "uclv.edu.cu" {
        type slave;
        masters { 200.55.145.10; };
        file "slaves/uclv.edu.cu";
};
```

Anexo 9A. Registros de la zona directa udg.co.cu, para la vista externa del DNS. (Archivo /var/named/chroot/var/named/data/udg.co.cu)

```
$ORIGIN udg.co.cu.
$TTL    86400
@       IN      SOA     mediaserver.udg.co.cu. root.udg.co.cu.  (
                                        2007062200 ; Serial
                                        28800      ; Refresh
                                        14400      ; Retry
                                        3600000    ; Expire
                                        86400 )    ; Minimum
                IN      NS      mediaserver.udg.co.cu.
                IN      MX      10      mail.udg.co.cu.
                IN      A       200.14.53.4
                IN      AAAA    2001:b00:f80b:0:0:0:0:4
cisco2811       IN      A       200.55.149.9
cisco2811       IN      A       200.14.53.1
```

```
mail            IN      A       200.14.53.2
antares         IN      A       200.55.149.11
antares         IN      A       200.14.53.3
antares         IN      A       200.14.53.17
mediaserver     IN      A       200.55.149.12
mediaserver     IN      A       200.14.53.4
proxy           IN      A       200.55.149.13
proxy           IN      A       200.14.53.5
jabber          IN      A       200.14.53.6
nostromo        IN      A       200.14.53.18
thot            IN      A       200.14.53.19

agronomia       IN      MX      10      mail.udg.co.cu.
contabilidad    IN      MX      10      mail.udg.co.cu.
humanidades     IN      MX      10      mail.udg.co.cu.
informatica     IN      MX      10      mail.udg.co.cu.
ingenieria      IN      MX      10      mail.udg.co.cu.
sum             IN      MX      10      mail.udg.co.cu.
veterinaria     IN      MX      10      mail.udg.co.cu.
sriocauto       IN      MX      10      mail.udg.co.cu.
scautocristo    IN      MX      10      mail.udg.co.cu.
sjiguani        IN      MX      10      mail.udg.co.cu.
sbayamo         IN      MX      10      mail.udg.co.cu.
syara           IN      MX      10      mail.udg.co.cu.
smanzanillo     IN      MX      10      mail.udg.co.cu.
scampechuela    IN      MX      10      mail.udg.co.cu.
smedialuna      IN      MX      10      mail.udg.co.cu.
sniquero        IN      MX      10      mail.udg.co.cu.
spilon          IN      MX      10      mail.udg.co.cu.
sbmaso          IN      MX      10      mail.udg.co.cu.
sbueyarriba     IN      MX      10      mail.udg.co.cu.
sguisa          IN      MX      10      mail.udg.co.cu.

quidway-ar-28-09-bayamo         IN      A       192.168.250.1
quidway-ar-28-09-bayamo         IN      A       192.168.0.1
ftp             IN      CNAME   mail
www             IN      CNAME   mail

intranet        IN      A       10.24.6.2
web             IN      CNAME   nostromo

asterisk        IN      CNAME   jabber
voip            IN      CNAME   jabber
cmap            IN      CNAME   jabber
router          IN      CNAME   cisco2811
quidway-bayamo  IN      CNAME   quidway-ar-28-09-bayamo
```

Anexo 9B. Registros de la zona directa udg.co.cu, para la vista interna del DNS. (Archivo /var/named/chroot/var/named/data/internal/udg.co.cu)

```
$ORIGIN .
$TTL 86400      ; 1 day
udg.co.cu               IN SOA  mediaserver.udg.co.cu. root.udg.co.cu. (
                                2007062217 ; serial
```

```
                                28800      ; refresh (8 hours)
                                14400      ; retry (4 hours)
                                3600000    ; expire (5 weeks 6 days 16
hours)
                                86400      ; minimum (1 day)
                                )
                        NS      mediaserver.udg.co.cu.
$TTL 600        ; 10 minutes
                        A       200.14.53.4
                        A       200.14.53.19
                        A       200.55.149.12
$TTL 86400      ; 1 day
                        MX      10 mail.udg.co.cu.
                        AAAA    2001:b00:f80b::4
$ORIGIN _msdcs.udg.co.cu.
$TTL 600        ; 10 minutes
0258f71e-0e6b-48e8-93b8-7cf663457c9a CNAME thot.udg.co.cu.
3889f360-cbe8-44d2-adc4-5034240b7e5c CNAME thot.udg.co.cu.
$ORIGIN _tcp.Bayamo._sites.dc._msdcs.udg.co.cu.
_kerberos               SRV     0 100 88 thot.udg.co.cu.
_ldap                   SRV     0 100 389 thot.udg.co.cu.
$ORIGIN _tcp.Bayamo-II._sites.dc._msdcs.udg.co.cu.
_kerberos               SRV     0 100 88 thot.udg.co.cu.
_ldap                   SRV     0 100 389 thot.udg.co.cu.
$ORIGIN _tcp.dc._msdcs.udg.co.cu.
_kerberos               SRV     0 100 88 thot.udg.co.cu.
_ldap                   SRV     0 100 389 thot.udg.co.cu.
$ORIGIN _msdcs.udg.co.cu.
_ldap._tcp.7421c516-32ac-4621-ad9e-aba6c09daacb.domains      SRV 0 100
389 thot.udg.co.cu.
$ORIGIN _sites.gc._msdcs.udg.co.cu.
_ldap._tcp.Bayamo       SRV     0 100 3268 thot.udg.co.cu.
_ldap._tcp.Bayamo-II    SRV     0 100 3268 thot.udg.co.cu.
$ORIGIN gc._msdcs.udg.co.cu.
_ldap._tcp              SRV     0 100 3268 thot.udg.co.cu.
$ORIGIN _tcp.Bayamo._sites.udg.co.cu.
_gc                     SRV     0 100 3268 thot.udg.co.cu.
_kerberos               SRV     0 100 88 thot.udg.co.cu.
_ldap                   SRV     0 100 389 thot.udg.co.cu.
$ORIGIN _tcp.Bayamo-II._sites.udg.co.cu.
_gc                     SRV     0 100 3268 thot.udg.co.cu.
_kerberos               SRV     0 100 88 thot.udg.co.cu.
_ldap                   SRV     0 100 389 thot.udg.co.cu.
$ORIGIN _tcp.udg.co.cu.
_gc                     SRV     0 100 3268 thot.udg.co.cu.
_kerberos               SRV     0 100 88 thot.udg.co.cu.
_kpasswd                SRV     0 100 464 thot.udg.co.cu.
_ldap                   SRV     0 100 389 thot.udg.co.cu.
$ORIGIN _udp.udg.co.cu.
_kerberos               SRV     0 100 88 thot.udg.co.cu.
_kpasswd                SRV     0 100 464 thot.udg.co.cu.
$ORIGIN udg.co.cu.
$TTL 86400      ; 1 day
agronomia               A       10.24.1.12
                        MX      10 mail
antares                 A       200.14.53.3
                        A       200.55.149.11
                        AAAA    2001:470:1f06:239::2
```

```
                        AAAA    2001:470:1f07:239::1
                        AAAA    2001:b00:f80b::3
                        AAAA    2001:b00:f80b:3::1
                        AAAA    2001:b00:f80b:4::4
asterisk                CNAME   mediaserver
$TTL 1200       ; 20 minutes
cheche-ii               AAAA    2001:b00:f80b:1:201:80ff:fe04:a883
$TTL 86400      ; 1 day
cisco2811               A       200.14.53.1
                        A       200.55.149.9
                        AAAA    2001:b00:f80b::1
cmap                    CNAME   jabber
contabilidad            A       10.24.1.13
                        MX      10 mail
                        AAAA    2001:b00:f80b:200::d
coppermine              A       10.24.6.18
                        AAAA    2001:b00:f80b:204::12
$TTL 600        ; 10 minutes
DomainDnsZones          A       200.14.53.19
$ORIGIN _sites.DomainDnsZones.udg.co.cu.
_ldap._tcp.Bayamo       SRV     0 100 389 thot.udg.co.cu.
_ldap._tcp.Bayamo-II    SRV     0 100 389 thot.udg.co.cu.
$ORIGIN DomainDnsZones.udg.co.cu.
_ldap._tcp              SRV     0 100 389 thot.udg.co.cu.
$ORIGIN udg.co.cu.
$TTL 86400      ; 1 day
electra                 CNAME   elektra
elektra                 A       10.24.1.1
                        A       10.24.6.1
                        A       192.168.4.1
                        A       192.168.251.2
                        AAAA    2001:b00:f80b:200::1
                        AAAA    2001:b00:f80b:3::2
                        AAAA    2001:b00:f80b:204::1
                        AAAA    2001:b00:f80b:208::1
email                   A       10.24.1.11
                        AAAA    2001:b00:f80b:200::b
$TTL 600        ; 10 minutes
ForestDnsZones          A       200.14.53.19
$ORIGIN _sites.ForestDnsZones.udg.co.cu.
_ldap._tcp.Bayamo       SRV     0 100 389 thot.udg.co.cu.
_ldap._tcp.Bayamo-II    SRV     0 100 389 thot.udg.co.cu.
$ORIGIN ForestDnsZones.udg.co.cu.
_ldap._tcp              SRV     0 100 389 thot.udg.co.cu.
$ORIGIN udg.co.cu.
$TTL 86400      ; 1 day
ftp                     CNAME   mail
ftpint                  CNAME   intranet
gecon                   A       192.168.4.2
hercules                A       10.24.1.2
                        AAAA    2001:b00:f80b:200::2
humanidades             A       10.24.1.17
                        MX      10 mail
                        AAAA    2001:b00:f80b:200::11
ict                     A       10.24.6.16
                        AAAA    2001:b00:f80b:204::10
informatica             A       10.24.6.14
                        MX      10 mail
```

```
                        AAAA    2001:b00:f80b:200::e
ingenieria              A       10.24.1.15
                        MX      10 mail
                        AAAA    2001:b00:f80b:200::f
intranet                A       10.24.6.2
                        AAAA    2001:b00:f80b:204::2
intranet2               CNAME   zeo
jabber                  A       200.14.53.6
                        AAAA    2001:b00:f80b::6
$ORIGIN jabber.udg.co.cu.
aim                     CNAME   jabber.udg.co.cu.
client                  CNAME   jabber.udg.co.cu.
conference              CNAME   jabber.udg.co.cu.
http                    CNAME   jabber.udg.co.cu.
freenode.irc            CNAME   jabber.udg.co.cu.
jud                     CNAME   jabber.udg.co.cu.
msn                     CNAME   jabber.udg.co.cu.
$ORIGIN msn.jabber.udg.co.cu.
conference              CNAME   jabber.udg.co.cu.
$ORIGIN jabber.udg.co.cu.
public                  CNAME   jabber.udg.co.cu.
users                   CNAME   jabber.udg.co.cu.
yahoo                   CNAME   jabber.udg.co.cu.
$ORIGIN udg.co.cu.
$TTL 10800      ; 3 hours
luis                    A       10.24.100.247
                        TXT     "31365ee45046673c43d711cb7d0eb06919"
$TTL 86400      ; 1 day
mail                    A       200.14.53.2
                        AAAA    2001:b00:f80b::2
mediaserver             A       200.14.53.4
                        A       200.55.149.12
                        AAAA    2001:b00:f80b::4
nostromo                A       200.14.53.18
                        AAAA    2001:470:1f07:239::2
odiseo                  A       10.24.6.19
                        AAAA    2001:b00:f80b:204::13
osiris                  A       10.24.1.5
                        AAAA    2001:b00:f80b:200::5
phraates                A       10.24.6.8
                        AAAA    2001:b00:f80b:204::8
proxy                   A       200.55.149.13
                        AAAA    2001:b00:f80b::5
proxy1                  A       10.24.1.16
                        AAAA    2001:b00:f80b:200::10
quidway-ar-28-09-bayamo         A       192.168.0.1
                        A       192.168.250.1
quidway-bayamo          CNAME   quidway-ar-28-09-bayamo
quidway-universidad     A       192.168.0.2
                        A       192.168.251.1
router                  CNAME   cisco2811
sbayamo                 A       10.25.6.2
                        MX      10 mail
sbmaso                  A       10.25.20.2
                        MX      10 mail
sbueyarriba             A       10.25.22.2
                        MX      10 mail
scampechuela            A       10.25.12.2
```

```
                        MX      10 mail
scautocristo            A       10.25.2.2
                        MX      10 mail
sguisa                  A       10.25.24.2
                        MX      10 mail
$TTL 1200       ; 20 minutes
sigenu                  A       200.14.53.21
$TTL 86400      ; 1 day
                        AAAA    2001:b00:f80b:200::e
sjiguani                A       10.25.4.2
                        MX      10 mail
smanzanillo             A       10.25.10.2
                        MX      10 mail
smaso                   CNAME   sbmaso
smedialuna              A       10.25.14.2
                        MX      10 mail
sniquero                A       10.25.16.2
                        MX      10 mail
spilon                  A       10.25.18.2
                        MX      10 mail
sriocauto               A       10.25.0.2
                        MX      10 mail
sum                     MX      10 mail
syara                   A       10.25.8.2
                        MX      10 mail
$TTL 1200       ; 20 minutes
thot                    A       200.14.53.19
$TTL 86400      ; 1 day
                        AAAA    2001:470:1f07:239::3
veterinaria             A       10.24.1.14
                        MX      10 mail
voip                    CNAME   jabber
web                     CNAME   nostromo
webagro                 CNAME   odiseo
webinf                  CNAME   odiseo
wpad                    A       200.14.53.4
www                     CNAME   mail
zeo                     A       10.24.1.127
```

Anexo 10A. Registros del archivo “9.3.2.0.7.0.f.1.0.7.4.0.1.0.0.2.ip6.arpa”, datos para la resolución inversa de la red interna de los servidores del nodo Bayamo. (Ubicado en /var/named/chroot/var/named/data/internal/ipv6rev/)

```
$TTL 86400
$ORIGIN 9.3.2.0.7.0.f.1.0.7.4.0.1.0.0.2.ip6.arpa.
@       IN      SOA     mediaserver.udg.co.cu. root.udg.co.cu. (
                        2007060100      ; serial
                        21600           ; actualiza después de 6 horas
                        3600            ; reintenta después de 1 hora
                        604800          ; expira en 1 semana
                        86400           ; TTL mínimo de 1 dia
                        )
```

```
        IN      NS      mediaserver.udg.co.cu.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     antares.udg.co.cu.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     nostromo.udg.co.cu.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     thot.udg.co.cu.
```

Anexo 10B. Registros del archivo "0.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa", datos para la resolución inversa de la red de los servidores del nodo de la Universidad. (Ubicado en /var/named/chroot/var/named/data/internal/ipv6rev/)

```
$TTL 86400
$ORIGIN 0.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa.
@       IN      SOA     mediaserver.udg.co.cu. root.udg.co.cu. (
                        2007060100      ; serial
                        21600           ; actualiza después de 6 horas
                        3600            ; reintenta después de 1 hora
                        604800          ; expira en 1 semana
                        86400           ; TTL mínimo de 1 dia
                        )

        IN      NS      mediaserver.udg.co.cu.

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     elektra.udg.co.cu.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     hercules.udg.co.cu.
5.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     osiris.udg.co.cu.
b.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     email.udg.co.cu.
c.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     agronomia.udg.co.cu.
d.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     contabilidad.udg.co.cu.
e.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     informatica.udg.co.cu.
f.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     ingenieria.udg.co.cu.
0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR     proxy1.udg.co.cu.
```

Anexo 10C. Registros del archivo "4.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa", datos para la resolución inversa de la red de pública o corporativa del campus universitario. (Ubicado en /var/named/chroot/var/named/data/internal/ipv6rev/)

```
$TTL 86400
$ORIGIN 4.0.2.0.b.0.8.f.0.0.b.0.1.0.0.2.ip6.arpa.
@       IN      SOA     mediaserver.udg.co.cu. root.udg.co.cu. (
                        2007060100      ; serial
                        21600           ; actualiza después de 6 horas
                        3600            ; reintenta después de 1 hora
                        604800          ; expira en 1 semana
                        86400           ; TTL mínimo de 1 día
                        )

        IN      NS      mediaserver.udg.co.cu.
```

```
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR    elektra.udg.co.cu.
2.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR    intranet.udg.co.cu.
0.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR    ict.udg.co.cu.
2.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR    coppermine.udg.co.cu.
3.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR    odiseo.udg.co.cu.
8.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0  IN   PTR    phraates.udg.co.cu.
```

Anexo 11A. Configuración del router multicast en antares.udg.co.cu (Archivo /usr/local/sbin/mrd.conf)

```
/* MRD example configuration file */

log {
        attach default "/var/log/mrd6/mrd6.log" extradebug;
}

mrib {
        prefix 2001:b00:f80b:200::/56 via 2001:b00:f80b:3::2;
}


/* Groups configuration */
groups {
        ff1e::/16 {
            pim {
                rp 2001:470:1f07:239::1;
            }
        }
}
```

Anexo 11B. Configuración del router multicast en elektra.udg.co.cu (Archivo /usr/local/sbin/mrd.conf)

```
/* MRD example configuration file */

log {
        attach default "/var/log/mrd6/mrd6.log" extradebug;
}

mrib {
    prefix 2001:470:1f07:239::/64 via 2001:b00:f80b:3::1;
    prefix default via 2001:b00:f80b:3::1;
}

/* Groups configuration */
groups {
        ff1e::/16 {
            pim {
                rp 2001:470:1f07:239::1;
            }
        }
}
```