UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACIÓN DE POSTGRADO
Maestría en Ciencias de la Computación

IMPLEMENTACIÓN DEL PROTOCOLO IPV6 EN LA INFRAESTRUCTURA DE RED DE DATO DE LA UCLA

JORGE GONZÁLEZ BRICEÑO

Barquisimeto, Abril 2011

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACIÓN DE POSTGRADO
Maestría en Ciencias de la Computación

IMPLEMENTACIÓN DEL PROTOCOLO IPV6 EN LA INFRAESTRUCTURA DE RED DE DATO DE LA UCLA

Trabajo de Grado presentado como requisito parcial para optar al grado de

Magister Scientiarum en Ciencias de la Computación

AUTOR: JORGE GONZÁLEZ BRICEÑO
TUTOR: JEAN PAUL ANGELI

Barquisimeto, Abril 2011

DEDICATORIA

A mi familia y a Colina.

Jorge

AGRADECIMIENTOS

A:

Dios, Divina Pastora.

Todos aquellos que aportaron sus conocimientos de alguna forma a este trabajo: Euvis Piña, Gennys Clemant, Luzneida Matute, Virginia Torres, Jean Paul Angeli, Junior Escalona, Luis Márquez, Gloria Galíndez, Francisco Reaño, Elías López, Luis Valero, William Polanco.

Al CENIT (en la persona de Gregorio Manzano), Conatel y LACNIC por la colaboración a través de sus técnicos y sistemas en el soporte para el anuncio hacia el exterior del protocolo IPv6.

INDICE

LISTA DE FIGURAS

LISTA DE CUADROS

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACIÓN DE POSTGRADO
Maestría en Ciencias de la Computación

IMPLEMENTACIÓN DEL PROTOCOLO IPV6 EN LA INFRAESTRUCTURA DE RED DE DATO DE LA UCLA

Autor: Jorge González Briceño

Tutor: Jean Paul Angeli

RESUMEN

Esta investigación tuvo como objetivo principal la implementación del protocolo IPv6 en la infraestructura de red de dato de la UCLA. La misma se desarrolló bajo la modalidad de proyecto factible apoyado en la investigación de campo y documental. La evolución al protocolo IPv6 proporciona varias ventajas en comparación con IPv4 y aislarse de tal realidad constituye una debilidad tecnológica. El agotamiento futuro de direcciones IPv4 públicas en la UCLA y a nivel mundial crea la necesidad de utilizar bloques de direcciones IPv6 para permitir el avance de servicios y aplicaciones. Se realizaron los diagnósticos de hardware, software, proveedores y recurso humano concluyendo la factibilidad técnica, operativa y económica para la implementación de IPv6. Para el desarrollo de la investigación se siguió un esquema de planificación de tareas con la finalidad de separar y ordenar las actividades ejecutadas. Se realizó una comprobación de hardware enmarcado en la topología de red tomando en cuenta la conectividad con los proveedores de servicio. Para los sistemas operativos, se ejecutaron las tareas de actualización y configuraciones para el soporte del protocolo IPv6 sirviendo de base para las configuraciones de servicios de red importantes en la infraestructura como DNS, DHCPv6 y Web. Se realizaron cambios en la seguridad de servidores (ip6table), listas de acceso (acl), zonas DMZ's e intervlan routing con el objetivo de continuar el esquema que ya se implementa para el protocolo IPv4 en los servidores y los accesos en la intranet, hacia y desde Internet. Con el apoyo de los proveedores de servicio anunciando el prefijo, registrando los DNS y obteniendo la delegación inversa, se consiguió la posibilidad de comunicación desde la UCLA, utilizando el protocolo IPv6, hacia y desde Internet.

Descriptores: Implementación del Protocolo IPv6, Dual Stack, Internet, IPv6, Redes de dato, Servicios de red, DNS.

INTRODUCCION

Entre las instituciones que forman parte del proyecto Reacciun2 se encuentran: la UCLA, UDO, LUZ, UCV, UC, UNA, UBA, IVIC, UPEL, USB, ULA, OPSU, FUNDCITE, entre otras. Cada una de ellas cuenta con una asignación de direcciones IPv6 con la finalidad de evolucionar al nuevo protocolo, promover el desarrollo de redes de altas prestaciones, unir a las instituciones académicas, científicas y tecnológicas y ponerlas al servicio de la comunidad científica y de investigación. De allí la necesidad de proponer la implementación del protocolo IPv6 en la infraestructura de comunicaciones de la red de la UCLA como un paso importante en la transición hacia la nueva Internet.

Según P. Grossetete (2008), la versión 6 del protocolo IP (IPv6) se desarrolló para resolver los problemas de IPV4 y ofrecer nuevas posibilidades a la evolucionante Internet. IPv6 proporciona grandes beneficios a los profesionales IT y a la red.

La adopción de IPv6 en el mercado estará dada por la habilidad de la arquitectura de acomodarse al crecimiento de Internet, las nuevas aplicaciones y servicios IP. Empresas e instituciones requieren iniciar el proceso de migración y determinar la manera de mantener la coexistencia durante la ventana de tiempo que llevará la transición global en el mundo. Éste es un proceso largo y complejo pero necesario e inevitable. IPv6 constituye la manera de garantizar el crecimiento sostenido de Internet en los próximos años.

En 1991 la fuerza de tareas de Internet (IETF) formó grupo de trabajo para analizar y dictar pautas para tratar los problemas del protocolo en relación al crecimiento de Internet. Según P. Grossetete y otros (2008), en 2001, IPv6 comenzó a ser integrado en productos comerciales como Sun Solaris 8, el sistema operativo de Cisco 12.2(2)T, Juniper JUNOS 5.1. Desde 1996 hasta 2006, la red llamada 6bone

sirvió de marco de pruebas de interoperabilidad.

Tal como anuncia el sitio web www.iana.org (2008), el espacio de direcciones de Internet es administrado por el IANA (autoridad de asignación de números de Internet) y el despliegue de direcciones IPv6 comenzó en 1999. Las direcciones IPv4 e IPv6 son asignadas de manera jerárquica, de forma que los usuarios finales obtienen direcciones de sus proveedores de servicio (ISP), los ISP reciben asignaciones de los registros regionales de Internet (RIRs) de acuerdo a las políticas de distribución y delegación. Los recursos de numeración de Internet para la región de Latinoamérica y el Caribe están a cargo de "LACNIC" (Registro de direcciones de Internet para América Latina y el Caribe), en Venezuela la red Académica de Centros de Investigación y Universidades Nacionales (Reacciun) es un proyecto que busca proveer a las instituciones académicas, científicas y tecnológicas de los recursos para desarrollar nuevas tecnologías en la futura generación de Internet, como aparece reseñado en el sitio *www.reacciun2.edu.ve.*

El trabajo se ha estructurado por capítulos que se describen a continuación:

Capítulo I, denominado planteamiento del problema, describe los objetivos de la investigación: general y específicos, así como la justificación, importancia y alcances que posee el proyecto.

Capítulo II, presenta los antecedentes de la investigación que sirvieron de apoyo para el desarrollo del proyecto. Presenta además el marco teórico, en el cual se muestran los aspectos teóricos que sustentan la investigación.

Capítulo III, describe la metodología utilizada para el desarrollo del proyecto, se presentan los procedimientos ejecutados con la finalidad de obtener el resultado propuesto.

Capítulo IV, se describen los pasos seguidos en el desarrollo de la investigación apoyado en las bases teóricas.

Capítulo V, se presentan una serie de conclusiones y recomendaciones como resultado de los procesos ejecutados a lo largo de la investigación.

CAPÍTULO I

EL PROBLEMA

Planteamiento del Problema

El 03 de Febrero de 2011 se anunció en LACNIC el agotamiento de direcciones IPv4 del stock central administrado por la IANA (Internet Assigned Numbre Authority) y se entregaron los últimos bloques disponibles de IPv4 a cada uno de los Registros Regionales de Internet. Dado el éxito de Internet se espera que las direcciones IPv4 se agoten en los próximos años. Se ha observado el crecimiento de dispositivos que necesitarán una o más direcciones IP para conectarse a Internet y las 4 mil millones de direcciones que permite el protocolo IPv4 no serán suficientes. El protocolo IPv6 dispone de un espacio de direcciones mucho mayor así como mejor capacidad de enrutamiento, seguridad, soporte a dispositivos móviles, multicast y constituye la solución al problema de agotamiento y estancamiento en caso de la no adopción.

Tal como se indica en su sitio web, el proyecto REACCIUN2 (Red Académica de Centros de Investigación y Universidades Nacionales), interconecta a las Universidades nacionales y centros de investigación con redes internacionales experimentales de Internet de alta velocidad en todo el mundo. También contempla la instalación de laboratorios en instituciones para la capacitación de talento humano (investigadores, docentes, y estudiantes) que promueven la investigación en distintas áreas (Telecomunicaciones, Medicina, Ingeniería Civil, Matemáticas, entre otras). El ente encargado de este proyecto es el Centro Nacional de Innovación Tecnológica (CENIT) en compañía de Universidades como la UCLA, ULA, UCV, UC, USB, UDO la UPEL y el IVIC, entre otros.

En la actualidad, la Universidad Centroccidental Lisandro Alvarado (UCLA), cuenta con una conexión correspondiente a la topología nacional del proyecto REACCIUN2 para interconexión con la red Internet2 a través del nodo del CENIT.

La UCLA posee una asignación de direcciones IPv6 hecha por el organismo encargado de otorgar dicho recurso en la región (LACNIC). Sin embargo, carece de una implementación del protocolo que permita la comunicación con otras Universidades y centros de investigación que cuentan con esa capacidad dentro y fuera del país.

Esta carencia limita así mismo la iniciativa de usar este protocolo para laboratorios de Investigación, equipos de Telemedicina, redes convergentes, y demás aplicaciones.

La escases de direcciones públicas IPv4 asignadas a la UCLA y su futuro agotamiento en función del aumento de servicios que puedan ser accedidos desde Internet, requiere de nueva asignación de este recurso.

En la actualidad, el bloque de direcciones IPv6 asignadas a la UCLA no se está utilizando, ya que se requiere de la implementación del protocolo a nivel de los equipos de red para proceder a planificar su despliegue.

La posibilidad de comunicación desde la UCLA con redes Académicas y de Investigación con conectividad del protocolo IPv6 nativo, sólo sería viable con la implementación de este protocolo.

Los factores citados anteriormente crean la necesidad de implementar el protocolo IPv6 en la infraestructura de redes de Dato de la UCLA aprovechando el recurso lógico y físico enmarcado en el proyecto REACCIUN2.

Surgen así, las siguientes interrogantes: ¿Cuál es el estado actual de la Red UCLA en relación al protocolo IPv6? ¿Cuáles son los pasos a seguir para la implementación del Protocolo IPv6 en la infraestructura de Redes de la UCLA? ¿Cuáles son los mecanismos de transición del Protocolo IPv4 a IPv6?

Responder a estos interrogantes conlleva al desarrollo de los siguientes objetivos:

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo General

Implementar el Protocolo de Internet versión 6 (IPv6) en la infraestructura de red de Dato de la Universidad Centroccidental Lisandro Alvarado (UCLA)

Objetivos Específicos

- Diagnosticar la situación actual de la infraestructura de redes de dato de la UCLA en relación a la implementación del protocolo IPv6.

- Determinar la factibilidad operativa, técnica, y económica para la implementación del protocolo IPv6 en la infraestructura de red de dato de la UCLA.

- Diseñar un plan de implementación del protocolo IPv6 en la infraestructura de Red de dato de la UCLA.

Justificación e Importancia

Tomando en consideración la relevancia de la investigación y docencia como actividades fundamentales en el ambiente Universitario, se hace necesario facilitar su avance y mantenimiento en el tiempo. Las tecnologías de información, específicamente la red, brinda actualmente un aporte importante para estas actividades en la UCLA. La tecnología evoluciona constantemente y en esa medida se observan mejoras en las aplicaciones y servicios aprovechables por los usuarios finales en diferentes ambientes, entre ellos el académico, en donde algunas de sus necesidades se ven beneficiadas con características disponibles en este protocolo, por ejemplo:

- El agotamiento de direcciones públicas IPv4 para servicios en la Red de la UCLA se resolvería con la asignación de direcciones IPv6 con las que cuenta la Universidad.
- El acceso a servicios desde la UCLA a sitios web, videoconferencia, p2p, telemedicina, etc., que se encuentren configurados con IPv6 nativo se podrá efectuar únicamente si se dispone de algún mecanismo de transición al nuevo protocolo ejecutándose en la infraestructura de comunicaciones local.
- El desarrollo de GRIDS en la UCLA se facilitaría con la disponibilidad de IPSEC como parte del Stack en IPv6.
- El incremento del espacio de direcciones públicas evitaría un estancamiento de servicios que requieran el acceso hacia y desde Internet.
- Aplicaciones de redes convergentes como VoIP en la Universidad tendrían un mejor soporte con la etiqueta de flujo incluida en la especificación de IPv6.
- Para redes móviles, el protocolo IPv6 incluye mecanismos mejorados para su implementación, aumentando las opciones para proyectos en redes inalámbricas en la UCLA.
- Aplicaciones como access grid y otras que requieren optimizar el uso del ancho de banda se ven beneficiadas con IPv6.
- Disponibilidad de IPSec como parte del stack, facilita el despliegue de aplicaciones que requieren seguridad de extremo a extremo, como disponibilidad de recursos en malla (grids).

Esta evolución no se efectúa de forma automática en los distintos elementos que forman la red de datos de la Institución, de allí la importancia de ejecutar la implementación de la nueva versión del protocolo de Internet (IPv6) en la infraestructura de red de la misma.

Alcances y Limitaciones

El desarrollo del trabajo propuesto consistió en realizar la implementación del protocolo Ipv6 en la infraestructura de red de Datos de la UCLA. Se diagnosticó el hardware y software de los dispositivos de Telecomunicaciones involucrados como routers, suiches, firewalls y de los equipos que ofrecen servicios de red como Dns, Dhcp, Web; permitiendo efectuar las configuraciones y cambios necesarios habilitando la disponibilidad del protocolo IPv6.

En relación a las limitaciones, es importante mencionar que en este trabajo no se encuentran incluidas todas las subredes de los usuarios finales dado que el mismo está orientado a los equipos de comunicaciones del Núcleo de la red (Core), seguridad y servicios principales de la red tanto perimetral como a nivel interno. En ese sentido, se incluyeron todas las redes DMZ's, subredes de Infraestructura, y dos subredes de nivel de acceso. Dada la disposición de una red totalmente conmutada, en caso de requerir el despliegue en uno o varios segmentos adicionales, se seguirá el mismo procedimiento de los segmentos ya configurados.

CAPITULO II

MARCO TEÓRICO

Antecedentes de la Investigación

El despliegue de la versión seis del Protocolo Ip, IPv6 en las redes Académicas y comerciales ha ido en aumento con la cercanía de la fecha probable del agotamiento definitivo de direcciones IPv4 para nuevas asignaciones. Las Universidades Venezolanas incluidas en el proyecto REACCIUN2 cuentan con recursos de importancia (Bloques de Direcciones IPv6) para iniciar la transición y a medida que se incorporen más Instituciones, habrá más recursos para la colaboración Interinstitucional en ese sentido. Algunos documentos de referencia, se nombran a continuación:

Gamess Eric (2007), en su trabajo "Implementación del Protocolo IPv6 en la UCV" presentó una solución al encarecimiento de direcciones Ipv4 públicas asignadas a la UCV que consistió en la migración al protocolo IPv6 realizando experimentos para comparar el desempeño TCP y UDP en IPv4 e IPv6, los cuales mostraron un similar comportamiento demostrando la factibilidad técnica para la transición al protocolo de nueva generación. Enfrentados a la escases de direcciones IPv4, se ejecutó la implementación de IPv6 en una topología similar a la red UCLA en la conexión con el proveedor de servicio de red académica describiendo los cambios requeridos en el desarrollo de ese proyecto. La similitud de topología a la red UCLA constituyó un importante aporte para el diagnóstico de las conexiones físicas y las posibles soluciones a desarrollar en la misma.

Jara Felipe (2009), en su trabajo de grado titulado "Estudio e Implementación de una red IPv6 en la Universidad Técnica Federico Santa María de Chile" realizó un estudio e implementación para la actualización de los equipos de la red junto al plan

de integración de IPv6, realizó además una revisión del soporte IPv6 en sistemas operativos y servicios de red, los protocolos de enrutamiento y su configuración en la topología de la red de esa Universidad. Se realizó un análisis de de los equipos de la infraestructura de red concluyendo que se requería actualizar el hardware en algunos casos. Se demostró necesaria la revisión exhaustiva de las alternativas para implementar una red con IPv6 aportando ejemplos para el desarrollo de un esquema de diagnóstico de hardware y software aplicables en la presente investigación

Schuh Sylvia (2006), desarrolló un trabajo de grado de nombre "Migrando Redes de Pequeños negocios a IPv6" en donde efectuó la migración IPv4 a Ipv6 de los servicios de red VoIP usando Asterisk, DHCP, DNS, Apache, Proxy, MySQL,, FTP, NTP, CUPS, MSN, IRC, Active Directory, Correo Electrónico, IPSEC6, SSH, VNC, TELNET, Ntop, Nmap, IPtables, MRTG, realizando un análisis de tales servicios en los sistemas operativos Windows y Linux, describiendo la configuración de los mismos, obteniendo como resultado una visión para la implementación en ambos sistemas. Constituyeron un importante aporte las explicaciones de pruebas realizadas para los diferentes servicios que también se implementarían en la red de la UCLA con IPv6, y en los sistemas operativos Windows y Linux a nivel de usuario final.

Prieto Jaime (2008), en su trabajo "Implementación de Appliances para enrutado de IPv6 desde plataformas hardware económicas" configuró un entorno IPv4-IPv6 de simulación de la red de datos de la Universidad Complutense de Madrid, con Dual Stack como mecanismo de transición efectuando un plan de direccionamiento distribuido en las diferentes Vlans de esa red utilizando el sistema operativo Linux. En este trabajo se planteó una forma de transición al nuevo protocolo usando el mecanismo dual stack. Se realizó una descripción de la planificación de direccionamiento IPv6 asignando a cada VLAn una red con prefijo /64 incluyendo aquellas consideradas estratégicas y dejando en espera aquellas que se consideraron innecesarias. Se planteó la importancia del soporte del protocolo en el hardware del backbone. Los elementos nombrados constituyeron una contribución importante para el inicio de la planificación de las subredes para IPv6 y el plan de

direccionamiento y segmentación con el mecanismo dual stack.

Todos los trabajos citados anteriormente sirvieron de base para esta investigación, por cuanto hacen notar la importancia que tiene la transición hacia el nuevo protocolo de Internet, los mecanismos para la misma, los elementos a tomar en cuenta, las ventajas en el mediano y largo plazo y su relación en las redes académicas.

Bases Teóricas

El Protocolo de Internet

El Protocolo de Internet (IP) provee un servicio de transporte de datagrama a través de la red. Este servicio no notifica al equipo final acerca de los paquetes perdidos debido a errores o por congestión de la red. Los datagramas IP contienen un mensaje o un fragmento del mismo, que puede ser de hasta 65535 bytes de longitud. El formato básico de la cabecera del paquete IP y las funciones de sus campos son las siguientes:

Versión: Especifica la versión del protocolo al que pertenece el datagrama. En la actualidad, la versión más utilizada es la 4.

Internet Header Length (IHL), 4 bits: Indica la longitud de la cabecera del datagrama en palabras de 32 bits (Word). El mínimo valor válido es cinco.

Differentiated Services, 8 bits: definido en el RFC 2474 obsolece el campo TOS (RFC1349). Permite al host originario diferentes clases de servicio para los paquetes que transmite. Codepoint corresponde a los seis bits más significativos y es denominado DSCP (DiffservCodePoint). Los enrutadores de borde de las redes clasifican y marcan los paquetes con el valos DSCP. Otros dispositivos de red en el núcleo (Core) utilizan el valor DSCP en la cabecera IP para seleccionar el comportamiento del paquete y proporcionar el tratamiento adecuado de Calidad de Servicio (QoS).

Total Length, 16 bits: Indica la longitud en bytes u octetos, del paquete entero, incluyendo cabecera y datos. El tamaño máximo de un paquete IP es de 64 KB o

65535 bytes. En la práctica, los tamaños de los paquetes son limitados por la máxima unidad de transferencia (MTU).

Identificación, 16 bits: Es utilizado para identificar fragmentos de un datagrama unos de otros. El módulo de protocolo originario de un datagrama de internet marca el campo identificación a un valor que debe ser único para ese par fuente-destino y protocolo para el tiempo que el datagrama esté activo en el sistema internet.

Flags: Es usado para fragmentación y re ensamblaje. El primer bit es llamado More Fragments (MF), y es utilizado para indicar el último fragmento de paquete tal que el receptor conozca que el paquete puede ser re ensamblado. El segundo bit es el de no fragmentar (DF), el cual suprime la fragmentación. El tercer bit no se utiliza.

Fragment Offset: Indica la posición del fragmento en el paquete original. En el primer paquete de una corriente de fragmentos, el Offset será de 0; en los siguientes fragmentos, este campo mostrará el offset en incrementos de 8 bytes.

Time 11 olive (TTL): Un valor de 0 a 255 indica el número de saltos que el paquete tiene permitido hacer antes de ser descartado en la red. Cualquier enrutador que vea este paquete, decrementará el valor de TTL en uno; si obtiene cero, el paquete será descartado.

Protocolo: Indica el protocolo de la capa más alta que contiene los datos que lleva el paquete, las opciones incluyen ICMP (1), TCP(6), UDP (17), OSPF (89).

Header Checksum: Porta información para asegurar la recepción de la cabecera IP sin errores. Este campo sólo chequea la cabecera IP, no el paquete entero.

Dirección IP Origen: Es la Dirección IP de 32 bits del host que envía el datagrama.

Dirección IP destino: Es la dirección de 32 bits del host destino para este datagrama.

Opciones: Es un campo variable y no es obligatoria su utilización, sin embargo, cualquier nodo debe ser capaz de interpretarlo. Puede contener un

número de opciones que tendrán dos posibles formatos: simple y compuesto.

Relleno: Utilizado para asegurar que el tamaño en bits de la cabecera es un múltiplo de 32. El valor usado es el 0.

Direccionamiento IP

Las direcciones IPV4 tienen una longitud de 32 bits. Se escriben como una secuencia de cuatro números representando el valor decimal de cada byte de la dirección. Como los valores son separados por puntos, la notación es referida como decimal punteada. Una dirección IP simple es 200.11.248.12. El protocolo IP utiliza las direcciones IP para identificar de forma única un host dado en Internet, o de manera general, en cualquier red. Una dirección IP identifica una interfaz que es capaz de enviar y recibir datagramas IP.

El problema del agotamiento de direcciones IPv4

El número de redes en Internet ha ido duplicándose anualmente durante años. Sin embargo, el uso de redes clase A, B y C difiere en gran medida. Casi la totalidad de las nuevas redes asignadas al final de los años 80 fueron clase B, en 1990 se hacía aparente que si continuaba esta tendencia, las últimas redes clase B se asignarían en 1994.

La razón de esta tendencia fue que los usuarios potenciales consideraron una Red Clase B como suficientemente grande para sus requerimientos anticipados porque permite utilizar 65534 hosts, mientras una red Clase C, con un máximo de 254 host, restringe severamente el potencial de crecimiento inclusive para una pequeña red en sus inicios. Además, existen relativamente pocas redes que requerirían 65536 direcciones en su totalidad y muy pocas para las cuales 254 es un límite adecuado. En resumidas cuentas, aunque las divisiones en Clase A, B y C son lógicas y fáciles de manejar, no son la forma más práctica porque las redes Clase C son muy pequeñas para ser útiles a la mayoría de las organizaciones mientras que las Clase B son muy

grandes para que las organizaciones ocupen todas las direcciones disponibles.

En Mayo de 1996, todas las direcciones Clase A estaban asignadas o consignadas, así como 61,95% de las Clase B y 36,44% de las direcciones IP Clase C. Las direcciones asignadas (Asigned) son aquellas que ya están en uso. Las direcciones consignadas (Allocated) incluyen las asignadas más aquellas redes que han sido reservadas por la IANA (por ejemplo las 63 direcciones Clase A reservadas) o destinadas a los registros regionales que subsecuentemente serán asignadas por esos registros.

A finales de 1990, las políticas de asignación de direcciones se modificaron para preservar el espacio de direcciones existentes, particularmente para evitar el agotamiento del espacio de direcciones Clase B.

Otro enfoque para la conservación del espacio de direcciones IP se describe en el RFC 1918. Este RFC reserva parte del espacio global de direcciones para ser utilizado en redes que no requieren conectividad a Internet. Estas redes típicamente son administradas por una sola organización. Los rangos reservados para este propósito son:

- 10.0.0.0: Una red Clase A.
- 172.16.0.0 hasta 172.31.0.0: 16 redes Clase B contiguas.
- 192.168.0.0 hasta 192.168.255.0: 256 redes Clase C contiguas.

Cualquier organización puede utilizar estas direcciones dentro de estos rangos. Sin embargo, como son direcciones que no son únicas globalmente, no están definidas para ningún router externo. Aquellos Routers en redes que no utilicen direcciones privadas, por ejemplo los ISP, se espera que descarten toda la información de enrutamiento relacionada con estas direcciones. Los Routers dentro de las organizaciones que usan direcciones privadas se supone que limitan todas las referencias a redes privadas a enlaces internos. No deberían anunciar externamente rutas privadas ni enrutar datagramas IP que contengan direcciones privadas a routers externos.

Los host que tienen direcciones IP privadas no poseen conectividad directa de

capa IP a Internet. Toda la conectividad a la internet externa debe ser proporcionada con aplicaciones de pasarela (proxy) o a través de NAT (Network Address Translation). NAT es conocido como enmascaramiento IP. Proporciona un mapa entre las direcciones IP internas y las externas oficialmente asignadas.

NAT (Traducción de Direcciones de Red)

Sólo un número pequeño de hosts en una red privada se comunica fuera de esa red. Si a cada uno de ellos se le asigna una dirección IP del grupo oficial únicamente cuando necesitan comunicarse, solo un pequeño número de estas es requerido. NAT puede ser una solución para redes con direcciones privadas que quieren comunicarse con equipos en Internet. Para cada paquete de salida, la dirección origen es comprobada por las reglas de configuración de NAT. Si la regla contiene la dirección origen, la misma es traducida a una dirección global del grupo de tales direcciones. El grupo de direcciones contiene aquellas direcciones que NAT puede usar para la traducción. Para cada paquete entrante, la dirección de destino es comprobada si está utilizada por NAT. Si es así, la dirección es traducida a la dirección interna original.

Las direcciones asignadas requieren ser reservadas en un grupo para que puedan usarse cuando se necesiten. Si las conexiones se establecen desde la red interna, NAT puede simplemente tomar la siguiente dirección pública libre en el grupo NAT y asignarla al host interno que la está solicitando. El servicio mantiene una huella de cuáles direcciones IP internas son mapeadas con cuáles direcciones Ip externas, de manera que es posible adaptar una respuesta desde la red externa en la correspondiente dirección IP interna.

Los NAT son traductores de cabecera IP y en particular, NAT es traductor de direcciones IP. La cabecera de un paquete IP contiene las direccione IP origen y destino. Si el paquete pasa de dentro hacia afuera, NAT reescribirá la dirección origen en la cabecera del paquete con un nuevo valor y alterará los checksums de las

cabeceras IP y TCP en el paquete al mismo tiempo para reflejar el cambio en el campo dirección. Cuando el paquete es recibido de afuera hacia adentro, la dirección destino es reescrita a un valor distinto, y de nuevo los checksums de las cabeceras IP y TCP son recalculados.

Limitaciones de NAT

No es posible para NAT ser completamente transparente a los dispositivos que lo usan. Existen problemas potenciales de compatibilidad que pueden presentarse si NAT no lleva a cabo algunas funciones que van más allá del simple intercambio de direcciones IP y posiblemente números de puerto en la cabecera IP. Aunque las direcciones IP supuestamente están en el dominio del protocolo IP, son realmente utilizadas por otros protocolos también, en la capa de red y en las capas superiores. Cuando NAT cambia la dirección IP en un datagrama IP, frecuentemente debe también cambiar direcciones en otros lugares para estar seguro de que las direcciones en varias cabeceras y cargas útiles, siguen siendo iguales. Estos problemas de compatibilidad requieren que aunque NAT debería trabajar teóricamente sólo en el nivel IP en la capa de red, en términos prácticos, los routers NAT deben estar "conscientes" de muchos más protocolos y llevar a cabo las operaciones especiales que se requieran. Algunas se requieren para todos los datagramas que son traducidos mientras otras sólo se aplican a ciertos datagramas y no a otros. Incluso cuando estas técnicas son añadidas a los routers NAT, algunas aplicaciones puede que no trabajen adecuadamente en un ambiente NAT.

Muchos protocolos de aplicación llevan direcciones IP en el protocolo de capa de aplicación. En estos casos, un Gateway de nivel de Aplicación (ALG) se requiere para completar la traducción. Por ejemplo:

- Muchos paquetes ICMP (por ejemplo "Destino Inalcanzable") llevan incrustados paquetes IP en la carga útil (payload) ICMP. Estos requieren traducción y regeneración de checksum.
- El protocolo FTP envía la dirección y asignación de puerto como información de texto en datagramas entre dispositivos durante la conexión. Un ALG FTP

se necesita para que NAT soporte FTP para buscar esta información y efectuar los cambios requeridos. La dirección a ser sustituida puede requerir más caracteres que la original, por ejemplo, 10.1.1.108 (10 caracteres ASCII) es remplazada por 190.45.10.23 (12 caracteres ASCII). Efectuar esta sustitución cambia el tamaño de la carga, esto significa que los números de secuencia TCP también deben ser modificados. En estas situaciones, NAT como tal asume cualquier trabajo adicional que sea necesario. Esta es una complicación que no ocurre sin el uso de NAT.

- Protocolos como H.323 usan múltiples conexiones TCP o corrientes de datos UDP para formar "sesiones empaquetadas". Si todas las conexiones en el "empaquetado" se originan del mismo sistema, se evita el ALG. Pero H.323 presenta otros retos, incluyendo puertos efímeros y direcciones IP codificadas ASN.1 incrustadas en la carga de aplicación.
- Los paquetes SNMP llevan direcciones IP que identifican trap origen e instancias de objetos. NAT dinámico hace imposible identificar únicamente host por direcciones IP, las direcciones públicas son transitorias y compartidas.
- Cuando IPSec se usa en modo transporte, la Cabecera de autenticación (AH) y la carga de seguridad encapsulada (ESP) utilizan una verificación de integridad que se basa en el valor de la carga completa. Cuando NAT trata de actualizar el checksum de TCP o UDP en el datagrama IP, este cambia el valor de los datos que el dispositivo receptor usa en el chequeo de la integridad AH o ESP. El chequeo fallará. Por tanto, NAT no se puede usar en modo transporte de IPSec. La manera más fácil de combinar IPSec con NAT es evitar estos problemas ubicando puntos IPSec en el espacio de direcciones públicas. Esto es, NAT antes de IPSec; no IPSec antes de NAT.

Enrutamiento sin Clases (CIDR Classless InterDomain Routing)

El enrutamiento IP estándar entiende solo Sólo direcciones de red Clase A, B

y C. Dentro de cada una de estas redes, se utilizan las subredes para proveer una mejor granularidad. Sin embargo, no hay manera de especificar que múltiples redes Clase C están relacionadas. El resultado es denominado el problema de la explosión de tablas de enrutamiento.

Tan pronto como Internet comenzó a crecer dramáticamente, surgieron algunos problemas con el esquema de direccionamiento por "Clases":

1. Carencia de flexibilidad en el direccionamiento interno.
2. Uso ineficiente del espacio de direcciones: la existencia de sólo tres bloques lleva al desperdicio del espacio limitado de direcciones IP.
3. Proliferación de entradas en las tablas de enrutamiento: Mientras Internet crece, se requieren más y más entradas para que los routers puedan manejar el enrutamiento de los datagramas IP lo cual causa problemas de desempeño en los mismos.

El desarrollo de IP versión 6 comenzó a mediados de los años 90 y se reconoció que tomaría años antes de su despliegue general fuera posible. Con la intención de extender la vida de IPv4 hasta que se completara la versión 6, fue necesario seguir un nuevo enfoque para el direccionamiento en los dispositivos IPv4. Este nuevo sistema elimina la noción de las clases de direcciones, creando un nuevo esquema de direccionamiento "Sin Clases" denominado Enrutamiento Inter Dominio sin Clases "Classless Inter-Domain Routing" o CIDR.

Este sistema se desarrolló a comienzos de los 90's y se formalizó en los RFC's 1517, 1518, 1519 y 1520. Este esquema trata los temas de direccionamiento y enrutamiento.

CIDR adapta el concepto de la división en subredes de una red a la Internet completa. En esencia, el direccionamiento sin clases significa que en vez de romper una red en subredes, se pueden agregar redes en "superredes" más grandes. En ocasiones CIDR es llamado supernetting por esta razón: aplica el principio de subredes a redes más grandes, la agregación de redes en superredes permite resolver el problema del crecimiento de las tablas de enrutamiento. Para

aplicar los conceptos de subredes a Internet entera, se necesita tener subredes de diferentes tamaños. CIDR es una aplicación a nivel de Internet no de subredes de un nivel sino de enmascaramiento de subredes de longitud variable (VLSM). Así como VLSM divide una red tantas veces como se quiera para crear subredes, sub-subredes, sub-sub-subredes, CIDR permite hacer lo propio con Internet entera, tantas veces como se necesite.

En teoría, CIDR provee a la autoridad central de asignación de direcciones, la flexibilidad de manejar bloques de direcciones de diferentes tamaños para las organizaciones basados en sus necesidades. Sin embargo, cuando CIDR se desarrolló, se hizo un cambio en el método por el cual se asignaban direcciones IP. Se manejan entonces bloques en forma jerárquica: se dividen grandes bloques en bloques más pequeños y a su vez en bloques aún menores y así sucesivamente. La Autoridad de Números Asignados de Internet (IANA) administra el fondo de direcciones unicast IPv4. El IANA no asigna direcciones a ISP's o usuarios finales, pero distribuye bloques de direcciones a los Registros Regionales (RIR's) bajo ciertos criterios definidos. El espacio de direcciones es distribuido a los RIR's en unidades de bloques /8 y es decisión de IANA los bloques específicos distribuidos al RIR. Cada Registro Regional distribuye direcciones a cada una de las regiones: Africa (AfriNIC), Asia Pacífico (APNIC), Norte América (ARIN), Latinoamérica y el Caribe (LACNIC) y Europa y el medio Este (RIPE NCC). Estos dividen los bloques de direcciones y los distribuyen a los Registros de Internet Nacionales de más bajo nivel (NIRs), Registros de Internet locales (LIRs) y a las organizaciones individuales tales como los proveedores de servicio (ISPs).

En la figura 1 se muestra la distribución de los registros regionales a nivel mundial.

Figura 1: Registros de Internet Regionales. **Fuente:** Arin.net

El Protocolo IPv6

El principal motivo por el que surge la necesidad de crear un nuevo protocolo en el IETF (Internet Engineering Task Force), fue la evidencia de falta de direcciones.

IPv4 cuenta con un espacio de direcciones de 32 bits, es decir, 2^{32} direcciones (4.294.967.296), aproximadamente 4000 millones. IPv6 ofrece un espacio de 2^{128} direcciones (340.282.366.920.938.463.463.374.607.431.768.211.456), aproximadamente 340 undecillones.

A principios de los años 70, los creadores de IPv4 no predijeron el éxito de este protocolo en el mediano plazo en una multitud de campos (científico, educación y vida cotidiana).

Dado el aumento de aplicaciones en las que se utiliza IPv4, se hizo necesario crear "parches" al protocolo básico, como: Calidad de Servicio (QoS), Seguridad (IPsec) y Movilidad. Sin embargo, surgieron inconvenientes cuando se requirió utilizar más de un "añadido" simultáneamente en estas ampliaciones en IPv4.

Principales Características de IPv6

Nuevo formato de Cabecera: El nuevo formato de cabecera se diseñó para minimizar el procesamiento de la cabecera, esto se lleva a cabo moviendo los campos opcionales y no esenciales a las cabeceras de extensión, ubicadas después de la cabecera IPv6. La cabecera IPv6 es procesada más eficientemente por los Routers

intermedios.

Las cabeceras IPv4 e IPv6 no son interoperables entre sí. Un host o Router debe usar una implementación de ambos protocolos para reconocer y procesar ambos formatos de cabecera. La cabecera por defecto IPv6 es únicamente del doble del tamaño de la cabecera IPv4 aunque el número de bits es cuatro veces mayor que una dirección IPv4.

Mayor espacio de direcciones: IPv6 posee 128 bits (16 Bytes). El espacio de direcciones de IPv6 se diseñó para permitir múltiples niveles de subredes y asignación de direcciones, desde el Backbone de Internet hasta las subredes dentro de una organización.

Configuraciones de direcciones modo Stateless y modo Stateful: IPv6 soporta la configuración de direcciones en presencia de un servidor DHCP para IPv6 (servidor DHCPv6) denominada Statefull, o en ausencia del mismo denominada configuración Stateless. En la configuración Stateless no se requiere la presencia de servidores de configuración que provean información a los hosts. Los Routers determinan los prefijos que identifican a la red asociada al segmento. El identificador de interfaz identifica una interfaz dentro de la subred y por defecto es generada a partir de la dirección MAC de la tarjeta de red. La dirección IPv6 se crea combinando los 64 bits del identificador de interfaz y el prefijo que el el Router tiene para esa subred. Si no hay router presente, el PC genera una dirección denominada link-local. Esta dirección resulta suficiente para comunicar varios nodos en el mismo segmento.

La configuración Statefull requiere un servidor que envíe información y parámetros de conectividad de red a los nodos. En general, este mecanismo se basa en el uso del protocolo DHCPv6. Statefull se emplea frecuentemente cuando se necesita un control riguroso en relación a las direcciones distribuidas a los hosts, en el caso de Stateless la preocupación consiste en que la dirección sea única.

Soporte de cabecera IPsec requerido: El soporte para cabeceras de IPsec es un requerimiento para la suite de protocolo IPv6. Este requerimiento proporciona una solución para las necesidades de protección de red. IPsec consiste de dos tpos de

cabeceras de extensión y un protoolo para negociar la configuración de seguridad. La cabecera de autenticación proporciona integridad de dato, autenticación de datos y protección de repetición para el paquete IPv6 (excluyendo los campos de la cabecera que deben cambiar en tránsito). La cabecera de carga de encapsulamiento de seguridad (ESP) proporciona integridad de dato, autenticación confidencialidad y protección de repetición para la carga ESP encapsulada. El protocolo que se usa típicamente para negociar las configuraciones de seguridad IPsec para comunicaciones unicast, es el protocolo de intercambio de llave de Internet (IKE).

Mejor soporte para envío prioritario: Existen en la cabecera de IPv6 campos nuevos que definen la manera como el tráfico es identificado y manejado. El tráfico se prioritiza usando el campo Traffic Class, el cual especifica un valor DSCP (Differentiated Services Code Point) tal como en IPv4. El campo Flow Label en la cabecera IPv6 le permite a los Routers identificar y manejar los paquetes que pertenecen a un flujo (definido somo una serie de paquetes entre un origen y un destino). Como el tráfico es identificado en la cabecera IPv6, se puede soportar el envío por prioridad inclusive cuando la carga útil esté encriptada con IPsec y ESP.

IPv6 restaura la comunicación fin a fin (end-to-end): con NAT en IPv4 existe una barrera técnica para las aplicaciones que dependen de la conectividad del par (peer) por la necesidad del par de comunicación de descubrir y anunciar su dirección IPv4 pública y sus puertos. Con IPv6, no se necesita NAT para conservar el espacio de direcciones públicas y para los desarrolladores de aplicaciones desaparecen los problemas relacionados con el mapeo de direcciones y puertos. Las comunicaciones end-to-end se restablecen entre hosts en Internet usando direcciones en paquetes que no se modifican en tránsito. Esto tiene un gran valor para la telefonía par a par, el video y otras tecnologías de colaboración en tiempo real en comunicaciones personales y en dispositivos que se conectan a Internet como teléfonos móviles.

Enrutamiento más eficiente con IPv6: contrario a IPv4, la cabecera de IPv6 es de tamaño fijo (40 Bytes), esto permite a los Routers procesar los paquetes UPv6 más rápido. Adicionalmente, la estructura jerárquica y resumible del direccionamiento

IPv6 significa que hay menos rutas que analizar en las tablas de enrutamiento de los Routers del backbone de Internet y de las organizaciones. Se tiene como consecuencia tráfico que puede ser reenviado a mayores velocidades resultando en un mejor desempeño.

IPv6 resuelve el problema de la distribución Internacional de Direcciones: En los inicios de Internet, los sitios conectados de Estados Unidos recibieron prefijos de direcciones IPv4 sin dependencia de la necesidad. Como consecuencia, este país posee un número desproporcionado de direcciones IPv4 públicas.

Con IPv6, los prefijos de direcciones públicas son asignados a los registros regionales, los cuales a su vez, asignan prefijos a otros ISP's y organizaciones basados en requerimientos justificados. Esta práctica asegura que los prefijos serán distribuidos globalmente basados en los requerimientos de conectividad regionales y no en orígenes históricos.

Direccionamiento IPv6

Los 128 Bits de la dirección IPv6 son divididos en límites de 16 bits y cada bloque de 16 bits se convierte en un número hexadecimal separado por dos puntos. Ejemplo:

0100 0000 0000 0001 0000 1101 1011 1000 0000 0000 0000 0000 0010 1111 0011 1011

0000 0010 1010 1010 0000 0000 1111 1111 1111 1110 0010 1000 1001 1100 0101 1010

Cada bloque de 16 bits es convertido a hexadecimal y delimitado por dos puntos resultando en la siguiente dirección:

2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A

La representación de la dirección de una dirección IPv6 se puede simplificar eliminando los ceros principales dentro de cada bloque de 16 bits. Suprimiendo los ceros principales, la dirección anterior queda de la siguiente manera:

2001:DB8:0:2F3B:2AA:FF:FE28:9C5A.

Compresión de ceros: Para las direccione IPv6 que contienen largas secuencias de ceros, la representación se puede simplificar comprimiendo 16 bits de ceros a doble dos puntos ::, por ejemplo, la dirección FE80:0:0:0:2AA:FF:FE9A:4CA2 se puede comprimir a FE80::2AA:FF:FE9A:4CA2; la dirección FF02:0:0:0:0:0:0:2 se puede comprimir en FF02::2. La compresión de ceros no se puede utilizar para incluir parte de un bloque de 16 bits, por ejemplo: FF02:30:0:0:0:0:0:5 no se puede expresar como FF02:3::5, sino como FF02:30::5.

Teniendo en cuenta que una dirección IPv6 está compuesta por 8 bloques de 16 bits cada uno, se puede determinar cuántos bloques de ceros están representados por el doble dos puntos::, restando 8 menos el número de bloques de la dirección ya comprimida. Por ejemplo: la dirección FF02::2 tiene dos bloques, restando 8 – 2 resultan 6, interpretándose que el número de bloques representados por los dos puntos es de 6 bloques. Para conocer la cantidad de bits representados por los dos puntos, se multiplica el número de bloques por 16, por ejemplo: en la dirección FF02::2, se multiplica 16x6=96 bits. La compresión de ceros se puede usar sólo una vez por cada dirección IPv6, de otra forma no se podría determinar el número de bloques de ceros o los bits representados por cada dos puntos::. Por ejemplo: 2001:0db8:0000:130f:0000:0000:087c:140b se puede representar como: 2001:db8:0:130f::87c:140b, los dobles dos puntos aparecen sólo una vez.

Prefijos IPv6: Los prefijos IPv6 representan los valores fijos de la dirección o los bits que definen una red o subred. Los prefijos IPv6 se escriben en el formato dirección/longitud del prefijo de la misma manera que en la notación CIDR.

Tipos de direcciones IPv6

Unicast: representa un simple interfaz en el ámbito del tipo de dirección. El ámbito es la región de la red IPv6 en la que la dirección es única.

Multicast: representa cero o más interfaces en el mismo o diferente host. En una topología de enrutamiento multicast apropiado, los paquetes direccionados a una dirección multicast son enviados a todas las interfaces identificadas por la dirección.

Una dirección multicast se usa para la comunicación uno a muchos, con entrega a multiples interfaces.

Anycast: Identifica multiples interfaces. Los paquetes direccionados a una dirección anycast son enviados a una sola interfaz (la más cercana que esté identificada por la dirección. Una dirección anycast se usa para comunicaciones uno a uno a muchos, con entrega a una sola dirección.

Especificaciones básicas de IPv6 en comparación con IPv4

En la figura 2 se muestra la descripción de la cabecera de un paquete IPv4.

Figura 2: Cabecera IPv4. **Fuente:** http://www.consulintel.es/

La longitud mínima de la cabecera IPv4 es de 20 Bytes (cada fila es de 4 bytes). A ello hay que añadir las opciones, que dependen en cada caso.

En color más claro se denotan los campos que son modificados y más oscuro, los que desaparecen, o que ya no existen en IPv6.

Existe una reducción de 12 campos en IPv4 a solo 8 en IPv6.

El principal motivo por el que los campos son eliminados, es la innecesaria redundancia. En IPv4 se provee la misma información de varias formas. Un caso evidente es el checksum o verificación de la integridad de la cabecera: otros mecanismos de encapsulado ya realizan esta función (IEEE 802 MAC, framing PPP, capa de adaptación ATM, entre otros).

En el caso del campo Fragment Offset (Desplazamiento de Fragmentación), el

mecanismo por el que se realiza la fragmentación de los paquetes es modificado en IPv6, lo que implica la total inutilidad de este campo. En IPv6 los routers no fragmentan los paquetes, sino que de ser requerida esta fragmentación/defragmentación, se produce extremo a extremo.

Algunos de los campos son renombrados:

- Longitud total: en IPv6 longitud de carga útil (payload length), que es la longitud de los propios datos y puede ser de hasta 65536 bytes. Tiene una longitud de 16 bits (2bytes).
- Protocolo: en IPv6 siguiente cabecera (next header), en lugar de usar cabeceras de longitud variables, se emplean sucesivas cabeceras encadenadas, de allí que desaparezca el campo de opciones. En muchos casos no es procesado por los routers, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).
- Tiempo de vida: en IPV6 límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1byte).

Los nuevos campos son:

- Clase de tráfico (Traffic Class), también denominado prioridad (Priority) o simplemente Clase (Class). Podría ser el equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1byte).
- Etiqueta de flujo (Flow Label), para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos son los que permiten una de las características de IPv6: Calidad de servicio (QoS), Clase de servicio (CoS) y un mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

La cabecera de un paquete IPv6 se observa en la figura 3.

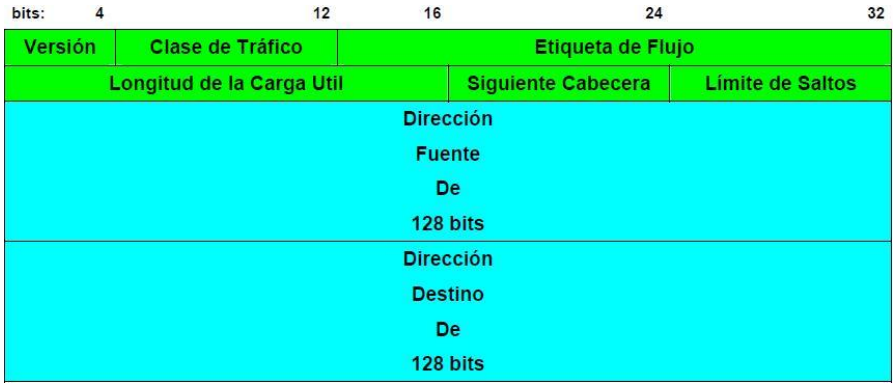

Figura 3: Cabecera IPv6. **Fuente:** http://www.consulintel.es/

La longitud de esta cabecera es te 40 bytes, el doble que el caso de IPv4, pero con la característica de haber eliminado campos redundantes.

La longitud fija de la cabecera, implica una mayor facilidad para su proceso en los routers y suiches, incluso mediante hardware, lo que implica mayores prestaciones.

El valor del campo siguiente cabecera (Next Header), indica cuál es la siguiente cabecera, las sucesivas cabeceras no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destino final. La única excepción a esta regla es cuando el valor de este campo es cero, indicando opción de examinado y proceso salto a salto (hop-by-hop). Se tiene por ejemplo, cabeceras con información de encaminado, fragmentación, opciones de destino, autenticación, encriptación, entre otros, que han de ser procesadas en el orden riguroso en que aparecen en el paquete.

A continuación, en la figura 4, unos ejemplos del uso del concepto de las cabeceras de extensión (definidas por el campo siguiente cabecera), mecanismo por el que cada cabecera es encadenada a la siguiente y anterior (si existen):

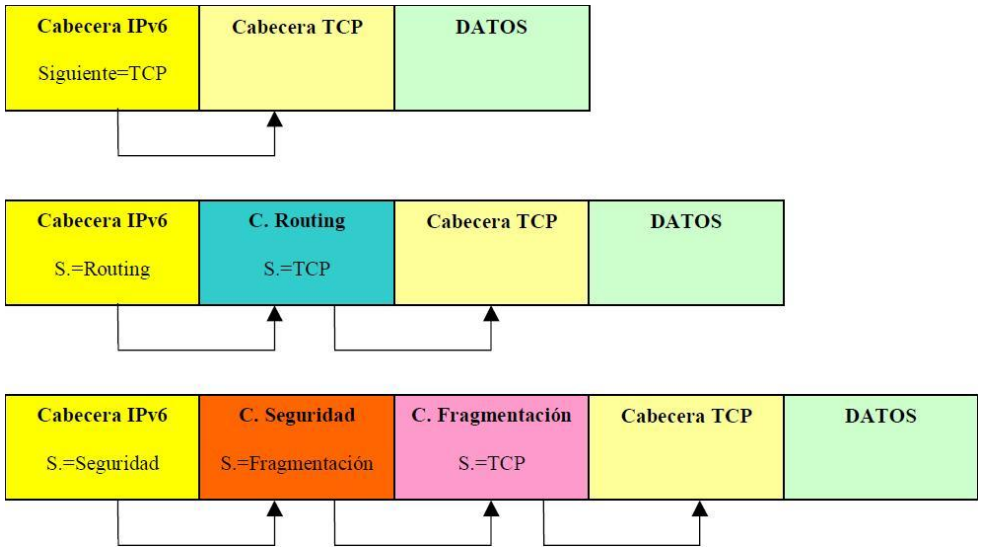

Figura 4: Cabecera de extensión. **Fuente:** http://www.consulintel.es/

Representación de las direcciones IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema:

- X:X:X:X:X:X:X:X donde X es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es obligatorio escribir los ceros a la izquierda de cada campo.
  Ejemplo: FEDC:BA98:7654:3211:FEDC:BA98:7654:3211

- Se permite la escritura abreviada de ceros mediante el uso de ::, que representa múltiples grupos consecutivos de 16 bits cero. Este símbolo sólo puede aparecer una vez en la dirección IPv6. Ejemplo:
  Las direcciones: 1080:0:0:0:8:800:200C:4174 (Una dirección Unicast)
  FF01:0:0:0:0:0:0:101 (Una dirección multicast)
  0:0:0:0:0:0:0:1 (La dirección Loopback)
  0:0:0:0:0:0:0:0 (Una dirección no especificada)
  Pueden representarse como:
  1080::8:800:200C:4174

FF01::101

::1 (La dirección de loopback)

:: (Una dirección no especificada

La representación de los prefijos IPv6 se realice del siguiente modo:dirección IPv6 / Longitud del prefijo, donde Dirección IPv6 es una dirección IPv6 en cualquiera de las notaciones válidas y la Longitud del prefijo es el valor decimal indicando cuántos bits contiguos de la parte izquierda de la dirección componen el prefijo. Por ejemplo:

- 2001:1338::/32
- 12AB:0000:0000:CD30:0000:0000:0000:0000/60
- 121AB::CD30:0:0:0:0/60
- 12AB:0:0:CD30::/60

IPv6 en el ambiente Académico

La adopción anticipada de IPv6 por parte de la comunidad académica ha tenido como resultado la experimentación e investigación y la formación de recursos humanos en el tema. Algunas necesidades del sector se ven beneficiadas con características disponibles en este protocolo.

- La necesidad de contar con direcciones públicamente alcanzables que permitan la interacción entre pares (en aplicaciones como videoconferencia, operación remota de instrumentos, entre otros)
- Características como multicast, necesario en aplicaciones como Access grid y otras que requieren optimizar el uso del ancho de banda.
- Disponibilidad de IPSec como parte del Stack, lo que facilita el despliegue de aplicaciones que requieren seguridad de extremo a extremo, como disponibilidad de recursos en malla.

- Las posibilidades que brindan las características de QoS incorporadas al protocolo.

Despliegue inicial CNTI[1]

- En el año 2004, posterior a la solicitud de bloques IPv6 a LACNIC, se asignó el bloque 2001:1338::/32.
- En el año 2005 LACNIC asigna el bloque 2800:30::/32
- En 2008: Conectividad nativa IPv6 Unicast a Red Avanzada a través de CLARA

En la figura 5 se observa el despliegue inicial de IPv6.

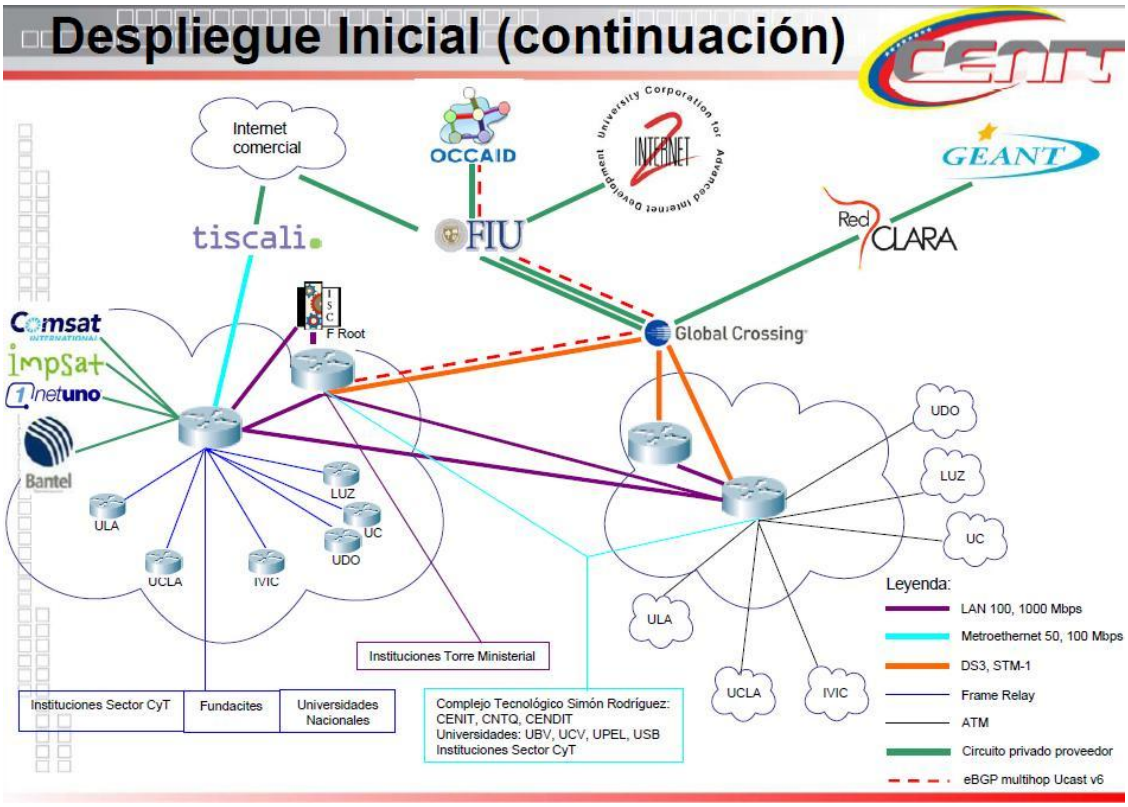

Figura 5:Diagrama del Despliegue inicial de IPv6. Fuente: lacnic.net

Plan de Direccionamiento Inicial IPv6 por parte del CNTI: Asignaciones

[1] *ipv6tour.lacnic.net/docs/f-obispo-implement-ipv6-cnti.pps*

- Bloques /48's para instituciones miembros de la Red Académica Nacional. Los bloques 2001:1338:FFFF::/48 y 2800:30:FFFF::/48 están reservados para conexiones punto a punto:
  Una /32: 65536 /48's = 65536 instituciones
- Bloques /64's para conexiones punto a punto:
  Una /48:65536 /64's = 65536 conexiones
- Bloques /128's para interfaces lógicas:
  Una /64: 18446744073709551616 identificadores

Redes Nacionales de Investigación y Educación

Una gran cantidad de países de todos los continentes pertenecen a las Redes Nacionales de Investigación y Educación (National Research and Education Networks, NRENS) en sus respectivas localidades. Las NRENS están formadas por instituciones académicas, centros de investigación, bibliotecas y entidades científicas comunicando a sus integrantes y propiciando la colaboración, innovación y cooperación en el conocimiento, fomentando el desarrollo de la tecnología de Internet, los servicios y la infraestructura a ser utilizados por la comunidad de investigación y educación.[2] Venezuela no escapa a esta realidad y el ente encargado de gestionarla es el Centro Nacional de Innovación Tecnológica CENIT.

Centro Nacional de Innovación Tecnológica CENIT

El 17 de Abril de 2006 se crea formalmente el CENIT mediante una alianza entre los Ministerios de la Defensa y Ciencia y Tecnología con la intención de brindar apoyo tecnológico a la empresa Venezolana de Industria Tecnológica VIT e impulsar la conformación de líneas de investigación para el desarrollo de las TIC en Venezuela, convirtiéndose en un espacio para la investigación, desarrollo e innovación. Entre sus objetivos se encuentra potenciar el desarrollo de la infraestructura de la Red Académica en conjunto con las redes sociales, integrar el

[2] http://www.terena.org/about/

conocimiento tecnológico nacional e internacional en función del desarrollo socioeconómico del País y contribuir a consolidar un sistema de investigación, desarrollo e innovación tecnológica que responda a las necesidades y requerimientos del mismo.[3]

Red Académica Nacional de Venezuela

La Red Académica de Centros de Investigación y Universidades Nacionales REACCIUN se originó a partir de una transformación del Sistema Automatizado de Información Científica y Tecnológica (SAICYT) por parte del CONICIT (Consejo Nacional de Investigaciones Científicas y Tecnológicas), reuniendo a las Universidades Nacionales y concretando los acuerdos para establecer la red. El SAICYT fue creado con la finalidad de atender las necesidades de información de la comunidad científica y tecnológica del país,[4] permitiendo el acceso a la información a instituciones, investigadores y público en general. Constaba de un sistema de conmutación de paquetes con una topología jerárquica con el nodo principal ubicado en Caracas y dos nodos secundarios en Barquisimeto y Puerto La Cruz. El nodo principal se conectaba a con la red Telenet de Estados Unidos, permitiendo el acceso a los servicios de información de Canadá, Estados Unidos y Europa Occidental.

Los aspectos fundamentales que pretendía cubrir el proyecto SAICYT eran:

1. Permitir el acceso automático a la información científica, tecnológica, técnica y económica publicada en el mundo.
2. Facilitar el intercambio de información entre científicos, técnicos y empresarios Venezolanos con sus colegas en el exterior.
3. Facilitar la organización y accesibilidad de la información generada en el país.
4. Permitir la interconexión de Centros de Investigación, Docencia y empresariales del país.

[3] http://portal.cenit.gob.ve/cenitcms/ noticia_2_1.html
[4] http://www2.reacciun.ve/reacciuncms/noticia_2322_1.html

En 1987 se terminaron de instalar los nodos y concentradores de la red en el territorio Nacional, diseñada para una base tecnológica X.25, firmándose un convenio con CANTV para la operación de la misma. Un enlace internacional disponía de un ancho de banda de 9600Bps.

Uno de los servicios fundamentales era el acceso a las bases y bancos de datos en el exterior, lo cual permitía obtener información publicada en otros países del mundo acerca de cualquier tema en particular. Se suscribieron convenios con Dialog Information Service INC, SDC-Search Service (Orbit) y Data France, entre otros, agregando posibilidades de acceso al universo de la información disponible en el mundo. Se cubrían áreas como: Medicina, Biología, ingeniería, Educación, Psicología, Sociología, Política, Economía, Directorios, Noticias, Negocios, etc.

En 1990 se instaló en el CONICIT un servidor con el sistema operativo UNIX, con la finalidad de ampliar los servicios de SAICYT. Se ofreció el servicio de correo electrónico en 1991 y se alcanzó un registro de 2mil usuarios pertenecientes a las comunidades académica y científica mediante una labor de promoción con universidades y centros de investigación. En 1993 se culminó el cambio de la plataforma X.25 a una red basada en protocolos TCP/IP.

En 1994, el CONICIT y 13 instituciones académicas llevaron a cabo la fundación de REACCIUN, que comenzó a operar formalmente en 1995. Para el año 1998 se incorporó la tecnología Frame Relay a la plataforma tecnológica de la red. REACCIUN es una Asociación Civil sin fines de lucro autorizada para su creación por Decreto Presidencial Nº 612, publicado en la Gaceta Oficial Nº 35691 de fecha 11 de Abril de 1995. En Marzo del año 2000, se creó el Centro Nacional de Tecnologías de Información (CNTI), el cual absorbió el capital humano y la plataforma tecnológica de servicios prestada por REACCIUN hasta esa fecha, modificando la adscripción, nombre y objeto de la asociación creada en 1995.[5]

Para el año 1998, REACCIUN tenía presencia en 14 ciudades del país de 13 Estados de Venezuela a través de las diferentes instituciones conectadas a la red:

[5] http://www.cnti.gob.ve/index.php?option=com_content&view=article&id=52&Itemid=60

Barquisimeto, Barinas, Coro, Caracas, Maracaibo, Mérida, Puerto Ordaz, Valera, Cumaná, La Victoria, Puerto La Cruz, Valencia y San Cristóbal. Algunas de las instituciones conectadas con enlaces a 64, 128 y 256 Kbps eran: **UCLA, CENAMEC, CIDA, CLAD, Conicit, IIBN, IICA, INCE, IVIC, LUZ, OPSU, UC, UCAB, UCV, UDO, UNA, UNEG, UNET, UNEXPO, UPEL, USB, UVM, IESA;** describiendo una topología que se en la figura 6:

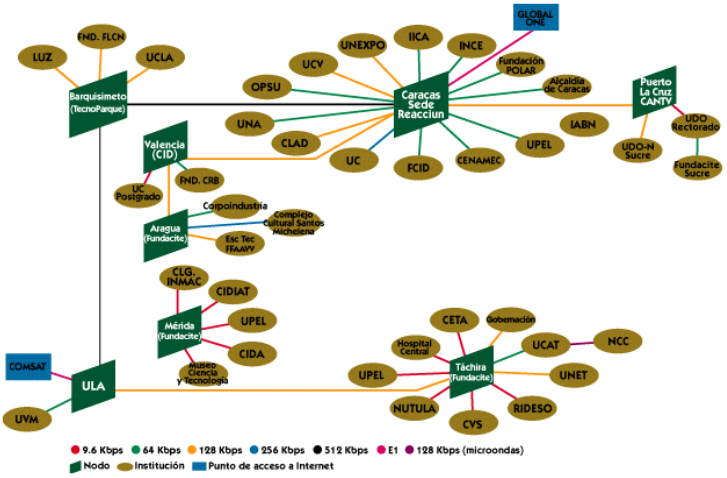

Figura 6: Topología de la red REACCIUN en 1998[6]. **Fuente:** http://neutron.ing.ucv.ve

Proyecto REACCIUN2

Los requerimientos de los usuarios del área de tecnología aumentan constantemente; la misma se va renovando en un esfuerzo por facilitar y mejorar sus aplicaciones y uso cotidiano. Las demandas de nuevos y mejores servicios, la intención de incorporar más nodos a la red, la necesidad de mayor ancho de banda que permita una calidad de servicio de voz, datos y vídeo en tiempo real así como otros recursos para conseguir una optimización de las actividades de los usuarios de la red Académica derivaron en la necesidad de iniciar un proceso de expansión y restructuración de la infraestructura de REACCIUN en un nuevo proyecto

[6] http://neutron.ing.ucv.ve/revista-e/No4/reacciun.htm

denominado REACCIUN2[7] (Red Académica de Centros de Investigación y Universidades Nacionales de Alta Velocidad). Consistió en la interconexión de 10 Universidades y un Centro e Investigación con las redes internacionales experimentales avanzadas. Las instituciones seleccionadas para formar parte de la red Reacciun2 (en una primera etapa) fueron la Universidad Centro Occidental Lisandro Alvarado, la Universidad de Los Andes, la Universidad Central de Venezuela, el Instituto Venezolano de Investigaciones Científicas, la Universidad de Carabobo, la Universidad de Oriente, la Universidad Simón Bolívar, la Universidad Pedagógica Experimental Libertador, la Universidad del Zulia, la Universidad Bolivariana de Venezuela y la Universidad Nacional Experimental de las Fuerzas Armadas. La infraestructura técnica que permitía la conexión fue provista por la empresa CANTV, encargada de realizar el transporte de señales entre las instituciones y el CNTI en una nube ATM.

El proyecto incluyó la dotación de enrutadores de borde, equipos de videoconferencia e instalación de laboratorios para capacitación e investigación, fortaleciendo la red académica de centros de investigación y Universidades Nacionales para su conversión a red de alta velocidad y sentando un precedente en relación al ancho de banda para cada Universidad y centro de investigación, permitiendo así mismo, la implementación de la nueva versión del protocolo IP (la versión 6), resultando una mayor flexibilidad, escalabilidad y enfoque progresista. Los anchos de banda con la mayoría de Universidades son de 34Mbps (a excepción de LUZ, UBV y UNEFA cada una con una disponibilidad inicial de 8Mbps). La conexión de la nube ATM se efectuó a través de dos canales de 155Mbps cada uno, enmarcados en el mismo convenio. La figura 7 muestra la topología inicial de Reacciun2.

[7] http://www.reacciun2.edu.ve/

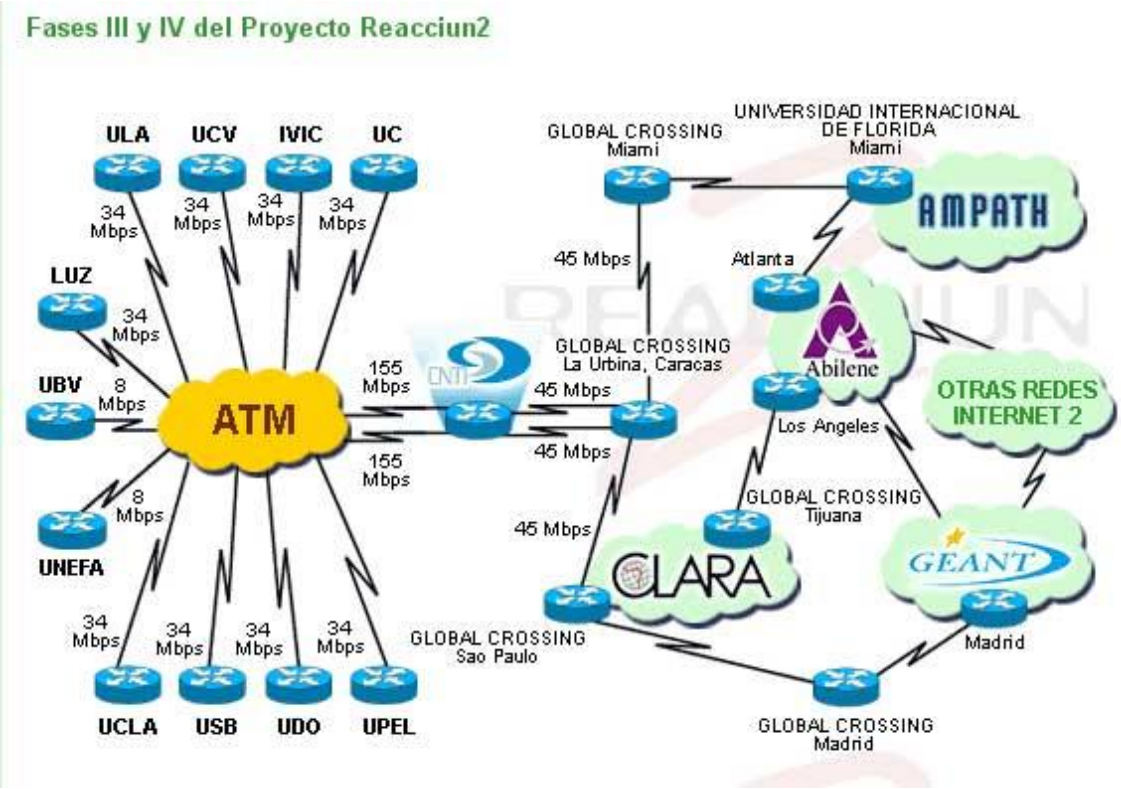

Figura 7: Topología inicial de la red REACCIUN 2. **Fuente**: http://www.reacciun2.edu.ve/

El proyecto REACCIUN2 buscaba la interconexión con redes avanzadas de Estados Unidos, Europa, América Latina y el resto del mundo; dedicadas exclusivamente a la educación, capacitación y proyectos de investigación que beneficiaran a los países participantes, no para fines comerciales. Una vez instalados los equipos de red así como la infraestructura que los soportara, se formarían grupos de trabajo por áreas de investigación: Videoconferencias, Tele-Salud, Tele-educación, Bibliotecas Digitales, Mallas Computacionales, Telecomunicaciones, entre otros, brindando a los sectores científicos y académicos la posibilidad de acceder a recursos en forma remota y participar en proyectos de colaboración multidisciplinarios, a nivel nacional o internacional. Para la comunicación internacional ya se disponía de una conexión hacia las redes avanzadas de Estados Unidos (por medio de un convenio con la Universidad de Florida (FIU)) y otra conexión hacia la Red CLARA para la conexión entre los países Latinoamericanos y otras redes a nivel mundial.En el año

2001, la Universidad Internacional de Florida (FIU) dio inicio al proyecto AMPATH (Americas Path) con el propósito de establecer una conexión de alta velocidad entre las redes de Educación e Investigación de Estados Unidos (ABILENE) y diez redes de Sur, Centro América, México y El Caribe. El proyecto AMPATH conectó desde Junio de 2001 hasta el año 2005, a las redes académicas de Chile (Reuna), Brasil (RNP), Venezuela (Reacciun) y Argentina (RETINA), así como a la Universidad de Puerto Rico. Esta red constituye un punto de interconexión de alto desempeño en Miami, Florida, el cual facilita el intercambio de tráfico y desarrollo de red entre Estados Unidos y las redes internacionales de investigación y educación. A través de su punto de intercambio, los servicios de red de alto ancho de banda están disponibles para Estados Unidos, Latinoamérica y el Caribe, mostrándose en la figura 8.

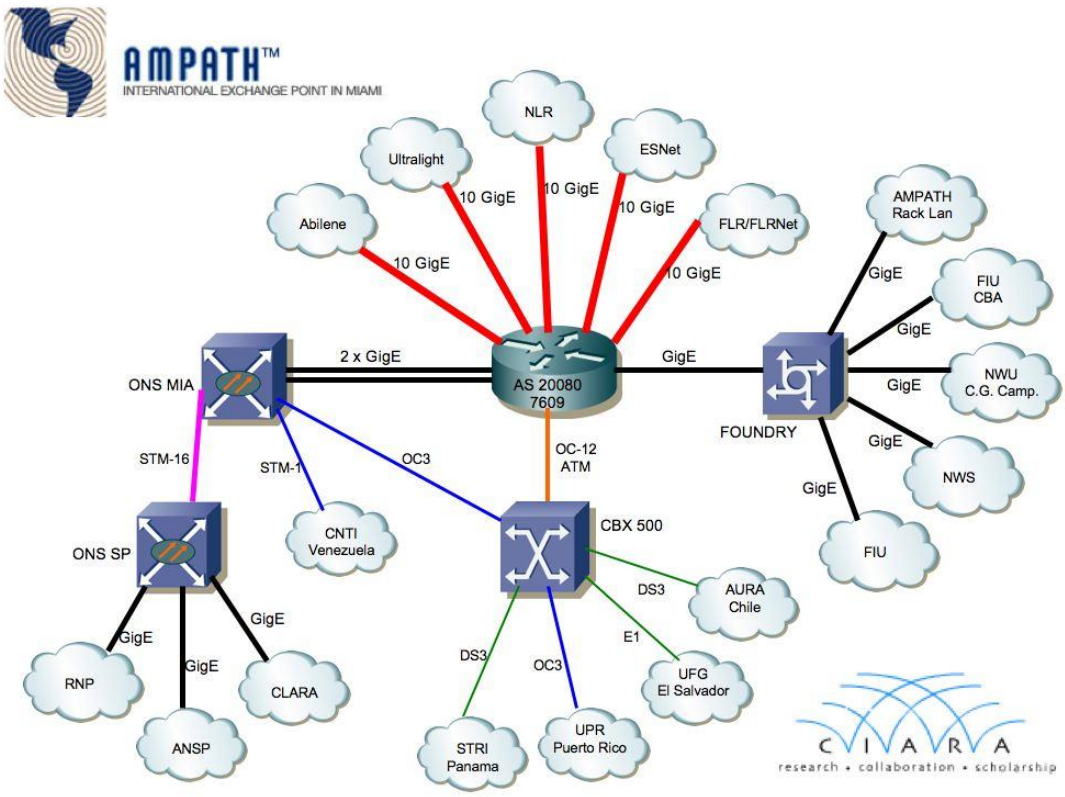

Figura8: Diagrama de la red AMPATH. **Fuente**: http://www.ampath.fiu.edu

En Abril de 2003, Reacciun se incorpora al proyecto AMPATH mediante un convenio con la Universidad de Florida (FIU), a través del cual se instaló un enlace de 45 Mbps proporcionado por la empresa Global Crossing para proveer la conectividad entre Reacciun y la red ABILENE en Estados Unidos. AMPATH es apoyada en parte por subvenciones de la Fundación Nacional de Ciencias de los Estados Unidos (NSF) como un proyecto colaborativo entre FIU y Global Crossing, usando una red de fibra óptica terrestre y submarina. Otra conexión internacional de la red académica Nacional Venezolana se efectúa a través de la red CLARA. Esta surge con la visión de crear una red troncal regional en América Latina y conectarla con la red de investigación y educación pan-europea (GÉANT).

GÉANT constituye el backbone que interconecta a las redes Nacionales de Investigación y Educación a través de Europa y proporciona conectividad mundial a través de enlaces con otras redes regionales. Los investigadores Europeos en campos como sismología, partículas físicas, pronóstico del tiempo y cambios climáticos requieren la disponibilidad de trabajar más cerca que nunca con sus contrapartes en el mundo. Adicional al alcance paneuropeo, la red GÉANT posee enlaces extensivos a redes en otras regiones del mundo, incluyendo Norte y Latinoamérica, los Balcanes, el Mediterráneo, Mar Negro, Asia Oriental y Central y está trabajando para conectar el Caribe y el sur de África.

Como consecuencia de su extenso alcance geográfico, alto desempeño, amplio ancho de banda y elevadas velocidades de transmisión, los investigadores de Europa están en la capacidad de compartir enormes cantidades de datos y colaborar efectivamente con sus colegas de todo el mundo, independiente de la distancia o la ubicación. En la figura 9 se muestra el diagrama de la red GEANT.

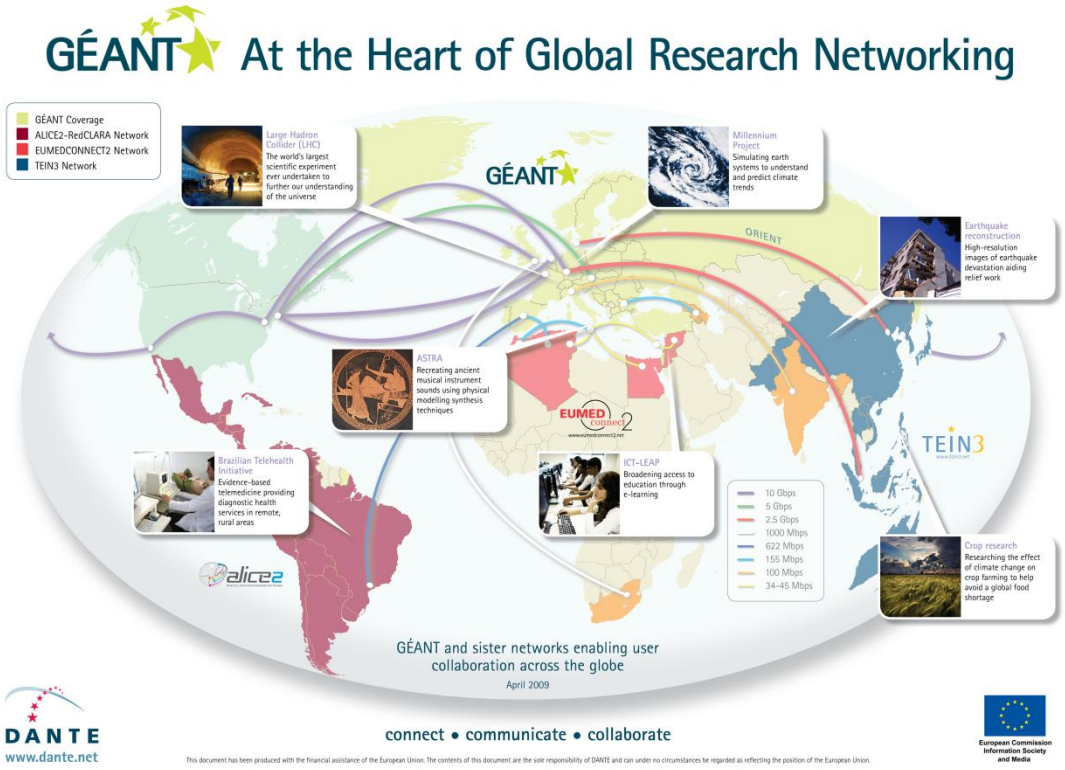

Figura 9: Diagrama de la red GEANT. **Fuente:** http://www.geant.net

La red GÉANT se enlaza a la red Latinoamericana CLARA a través de una conexión STM-4, a 622Mbps

En el año 2007 Reacciun pasa a ser miembro de la asociación LAUREN (Latin America University Research and Education Networks) a través de un convenio con la FIU en donde los miembros de Reacciun pueden tener acceso a la red Internet2. Con este convenio se actualizó el enlace entre Reacciun e Internet2 a 105Mbps.

La interconexión de las Redes Nacionales de Investigación y Educación

El grupo de protocolos TCP / IP es el método estándar de la industria para interconectar equipos, redes e Internet. Como tal, constituye el motor detrás de Internet y las redes alrededor del mundo. El principal objetivo de TCP/IP fue proveer

servicios de comunicación sobre redes físicamente heterogéneas. El beneficio de tal interconexión es la posibilidad de comunicación entre equipos en diferentes redes, separadas por ares extensas geográficamente.

Internet está constituido por los siguientes grupos de redes:

- Backbones: Grandes redes que existen principalmente para interconectar otras redes. Conocidos como NAPs o IXPs.
- Redes Regionales: conectan Universidades y Colegios, por ejemplo.
- Redes comerciales: Proveen acceso al backbone a suscriptores, y a redes pertenecientes a organizaciones comerciales que tienen conexión a Internet.
- Redes locales, tales como redes Universitarias de campus.

Otro aspecto importante de las inter redes TCP/IP consiste en la abstracción estandarizada del mecanismo de comunicación proporcionado por cada tipo de red. Cada red física posee su propia interfaz de comunicación, en la forma de interfaz de programación que proporciona funciones básicas de comunicación. TCP/IP provee servicios de comunicación que se ejecutan entre la interfaz de programación de la red física y las aplicaciones de usuario. Esto permite una interfaz común para estas aplicaciones, independiente de la capa física subyacente. La arquitectura de la red física está oculta para el usuario y para el desarrollador de la aplicación. La aplicación requiere sólo codificar a la abstracción de comunicación estandarizada para permitirse funcionar bajo cualquier tipo de red física y plataforma de operación. Para interconectar dos redes, se requiere un equipo que se encuentre conectado a ambas redes y que sea capaz de enviar paquetes de dato de una red hacia la otra, tal equipo se denomina enrutador o router. El término enrutador IP es también utilizado ya que la función de enrutamiento es parte de del protocolo IP en el grupo TCP/IP.

Para poder identificar un equipo dentro de una red, a cada uno se le asigna una dirección denominada dirección IP. En un enrutador, cada interfaz posee una

única dirección IP. La dirección IP consiste de dos partes: El número de red y el número de host.

El número de red, si la dirección es pública, identifica la red dentro de Internet y es administrada por una autoridad central.

El número de host especifica exactamente la interfaz del equipo al que se le asigna la dirección y es único en Internet (si es una dirección pública).

El grupo de protocolos TCP/IP está modelado en capas. Esta representación lleva al término "pila de protocolo", el cual se refiere a la pila de capas en el protocolo. Se puede usar para posicionar (no para comparar funcionalmente) a TCP/IP contra otros, tal como el modelo OSI. Las comparaciones funcionales no pueden extraerse fácilmente ya que existen diferencias básicas en los modelos de capas utilizados en los diferentes grupos de protocolos.

Con la división del software de comunicación en capas, la pila de protocolos permite la división de tareas, fácil implementación y pruebas del código. Una capa provee servicio a directamente superior y hace uso de los servicios proporcionados por la capa inmediatamente inferior. Por ejemplo, la capa IP provee la habilidad de transferir datos de un host hacia otro sin ninguna garantía de entrega confiable ni eliminación de duplicados. Los protocolos de transporte como TCP hacen uso de este servicio para proveer a las aplicaciones entrega del stream de datos con confiabilidad y en orden.

Capa de Aplicación: La capa de aplicación es proporcionada por el programa que utiliza TCP/IP para comunicación. Una aplicación es un proceso de usuario cooperando con otro proceso usualmente en otro equipo. Ejemplos de aplicación incluyen Telnet, Ftp. La interfaz entre las capas de aplicación y transporte está definida por los números de puerto sockets.

Capa de Transporte: Provee transferencia de datos fin a fin, entregando datos de una aplicación a su par remoto. El protocolo de capa de transporte más usado es TCP, el cual provee entrega de datos confiable orientada a conexión, con supresión de duplicado de datos, control de congestión y control de flujo. Otro protocolo de la capa de transporte es UDP. Este no es orientado a conexión, no es

confiable, y provee servicio del mejor esfuerzo. Como resultado, las aplicaciones que utilizan UDP como protocolo de transporte, tienen que proporcionar su propio mecanismo de integridad, control de flujo, control de conexión si lo desean. Usualmente, UDP es utilizado por aplicaciones que requieren un mecanismo rápido de transporte que pueda tolerar la pérdida de algunos datos.

Capa de Internet: También llamada la capa de Red. El protocolo más importante en esta capa es el Protocolo IP. No está orientado a conexión y no asume confiabilidad de otras capas. No proporciona confiabilidad, control de flujo, o recuperación de errores. Estas funciones deben ser proporcionadas por niveles superiores. IP provee función de enrutamiento que intenta entregar mensajes transmitidos a su destino. Un mensaje en una red IP es denominado Datagrama IP. Esta es la unidad básica de información transmitida a través de redes TCP/IP. Otros protocolos de capa de red son IP, ICMP, IGMP, ARP y RARP.

Capa de acceso a red: también llamada capa de enlace o capa de interfaz de red, es la interfaz al hardware de red. Es la responsable del formateo de los paquetes y la ubicación de los mismo en la red subyacente.

Estado actual de IPv4

IPv4 es un recurso limitado a un número fijo de 4,294,967,296 dispositivos conectados en su máximo teórico. El IANA es el cuerpo que mantiene el espacio de direcciones conteniendo 256 bloques de 16,777,216 (un /8) cada uno. 256 bloques multiplicados por 16,777,216 da como resultado 4,294,967,296; o 4.3 billones de direcciones IPv4 en total.

El IANA mantiene un fondo de direcciones no distribuidas, mientras que el resto ya han sido distribuidas a los RIR’s para su asignación subyacente. El estado actual del total del espacio de direcciones IPv4 se muestra en el siguiente gráfico. En la figura 10 se muestra el estado de IPv4 en el año 2010.

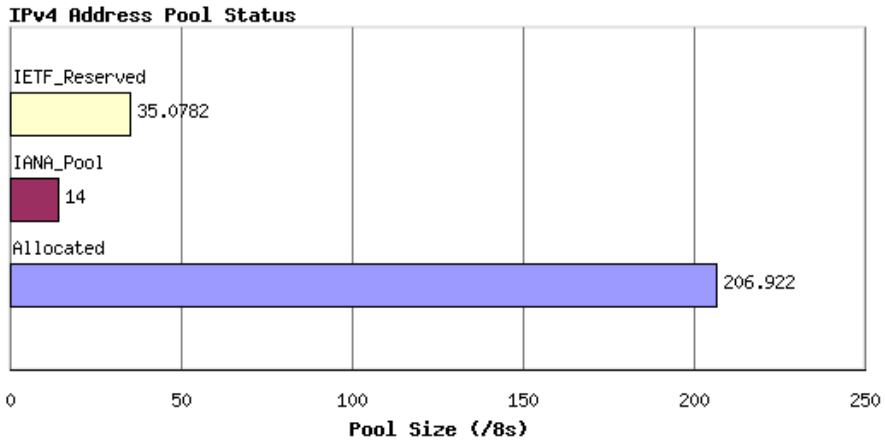

Figura 10: Estatus actual (2010) del espacio de direcciones IPv4. **Fuente:** http://www.potaroo.net

Cada uno de los cinco Registros Regionales (RIR's) toma espacio de direcciones IPv4 del IANA. Los RIRs utilizan entonces ese espacio de direcciones IPv4 para satisfacer las solicitudes de recursos en sus respectivas regiones. Un reporte del Registro Americano para Números de Internet (ARIN) muestra el espacio ya distribuido a los RIR's, cuál está disponible todavía y cuál no está disponible. El espacio de direcciones no disponible (mostrado en la figura 11) incluye las direcciones de multicast Clase D, el espacio experimental Clase E y el espacio identificado en el RFC 1918 (Asignación de direcciones para Internet Privadas).

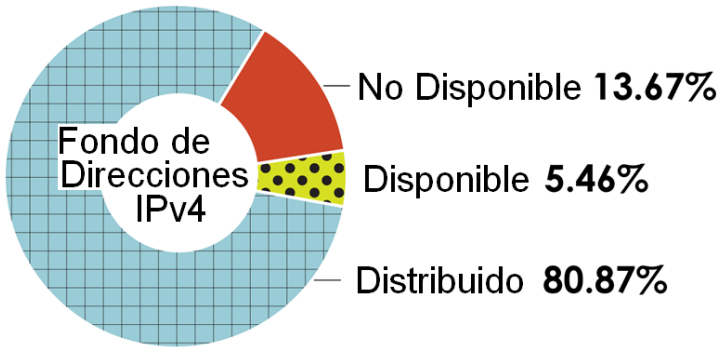

Figura 11:Uso del espacio de direcciones IPv4 al 6 de Agosto de 2010. **Fuente:** https://www.arin.net

El IANA distribuyó cuarenta /8s a los RIRs en los últimos cuatro años. Debido al incremento en la demanda, los RIRs posiblemente agotarán el fondo de direcciones IPv4 para finales de 2011. En el año 2010 a los RIR`s les ha sido distribuido doce /8s hasta el 6 de Agosto, dejando catorce /8 no distribuido (14 /256 = 5.46%), mostrándose en la figura 12.

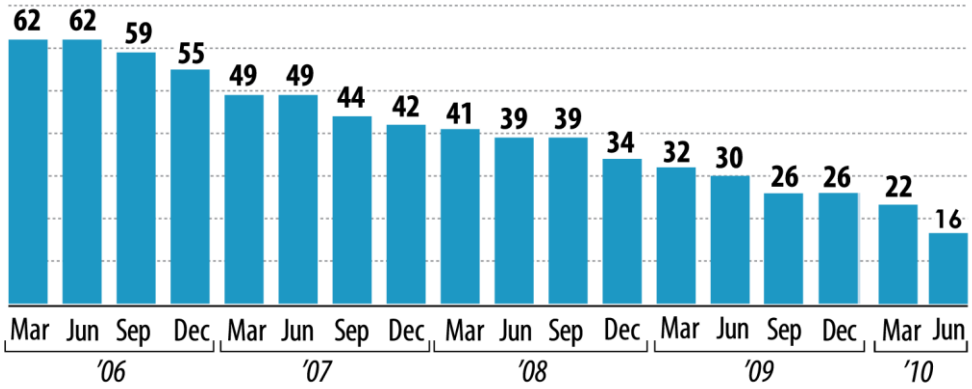

Figura 12:Espacio IPv4 Disponible en /8 en el tiempo. **Fuente:** https://www.arin.net

Las direcciones IPv4 son extraídas del fondo de direcciones no distribuidas, administradas por IANA. Estas distribuciones son hechas a los Registros Regionales de Internet (RIRs) y la unidad de distribución es en unidades de /8s.

Las actuales tendencias[8] predicen que las direcciones restantes que no han sido distribuidas aún por la IANA, se agotarán a mediados del año 2011 y para los RIRs a mediados del año 2012.

IPv4 ha existido por décadas y ha sobrevivido al crecimiento de Internet desde una pequeña red de investigación a una poderosa red global esparcida por el mundo, sin embargo, algunas limitaciones en el protocolo frenarían el crecimiento del tamaño de Internet así como los servicios. Los PC's de mano de hoy en día

[8] http://www.potaroo.net/tools/ipv4/

pueden hacer más que los más potentes servidores en el pasado. La cantidad de gente conectándose globalmente se ha incrementado de gran forma.

El principal problema de IPv4 es su relativamente pequeño espacio de direcciones de 32 bits. Probablemente se hubieran agotado para esta fecha las direcciones IPv4 bajo el esquema original de distribución de direcciones en "Clases". El cambio al direccionamiento "Sin Clase" y las tecnologías como NAT que permite a equipos con direcciones privadas acceder a Internet, han ayudado a posponer este hecho. El espacio de direcciones de 32 bits se hizo pequeño para el tamaño actual y futuro de Internet y la manera más conveniente de tratar este problema es cambiando a un espacio de direcciones mayor. Esta fue el principal factor en la creación de la siguiente versión del Protocolo de Internet, IPv6.

A continuación se muestran los cambios más importantes entre IPv4 e IPv6:

- Mayor espacio de direcciones: Las direcciones IPv6 poseen 128 bits de longitud en contraste de los 32 bits de IPv4. Esta característica expande el espacio de direcciones de aproximadamente 4 Billones de direcciones a cerca de 340 quintillones de direcciones.
- Espacio de direcciones jerárquico: Una de las razones por las que el tamaño de direcciones fue expandido tanto fue para permitir dividirse jerárquicamente para poveer un gran número de clases de direcciones.
- Asignación jerárquica de direcciones Unicast: Se creó un formato de direcciones unicast global para permitir distribuir fácilmente direcciones en todo Internet.
- Mejor soporte para direccionamiento no unicast: Se mejoró el soporte para multicast y se agrega soporte para el direccionamiento anycast.
- Renumeración y Auto configuración: se incluye una condición para facilitar la autoconfiguración y renumeración de direcciones IP en redes y subredes como se requiera.

---

http://ipv4depletion.com/?page_id=4

- Nuevo formato de Datagrama: Se redefinió el Datagrama IP otorgándosele nuevas capacidades.
- Soporte para Calidad de Servicio (QoS): Los Datagramas IPv6 incluyen características de QoS, permitiendo un mejor soporte para multimedia y otras aplicaciones que lo requieren.
- Soporte para Seguridad: El soporte para seguridad se diseñó dentro de IPv6 utilizando las cabeceras de extensión de encriptado, autenticación.

Otro cambio importante es que con la introducción de IPv6, otros protocolos TCP/IP se actualizaron. Uno de estos es ICMP, el protocolo de soporte más importante para IPv4 que fue revisado a través de la creación de ICMPv6 para IPv6. Otro adicional a TCP/IP es el Protocolo de Descubrimiento de Vecino (ND) el cual lleva a cabo varias funciones para IPv6 que realizaba ARP e ICMP versión 4.

La ventaja fundamental de IPv6 es el espacio de direcciones.

Una falta de coordinación en la delegación de direcciones en la década de los 80, está llevando al límite el agotamiento de direcciones.

La renumeración y reasignación del espacio de direcciones pudiera ser una solución, sin embargo, se requieren esfuerzos de coordinación a escala mundial que harían de este recurso una dificultad mayor. Por otro lado, la gran dimensión de las tablas de enrutamiento en el troncal de Internet que perjudica los tiempos de respuesta, permanecería como problema de IPv4.

La imposibilidad práctica de muchas aplicaciones que quedan relegadas a su uso en Intranets, dado que muchos protocolos no pueden atravesar los dispositivos NAT:

- RTP y RTCP (Real Time Protocol y Real Time Control Protocol) usan UDP con asignación dinámica de puertos (NAT no soporta esa traslación.
- La autenticación Kerberos requiere la dirección fuente, que es modificada por NAT en la cabecera IP.
- IPSec pierde integridad, debido a que NAT cambia la dirección en la cabecera IP.

- Multicast, aunque es posible técnicamente, su configuración es complicada y en la práctica no se emplea.

Un agotamiento de direcciones IP implicaría que Internet no podría seguir creciendo de la forma como lo ha venido haciendo hasta ahora y se dificultaría la incorporación de nuevos usuarios, dispositivos, servicios, aplicaciones y en general la innovación en Internet. El costo de desarrollo de software aumentaría así como el costo asociado al uso de Internet para nuevos servicios y aplicaciones.

Mecanismos de Transición a IPv6

Tal como se explica en el sitio http://portalipv6.lacnic.net/es/mecanismos-de-transici-n, en el diseño del ptotocolo IPv6 se especificó que debería coexistir con IPv4 y para lograr esta premisa se desarrollaron los mecanismos de transición. Estos se dividen en grupos diferenciados: Dual Stck, Traducción y túneles.

Dual Stack mantiene en simultáneo la pila del protocolo IPv4 y la de IPv6, pudiendo establecer comunicación y acceso a servicios dependiendo del protocolo del destino con el cual se trata de conectar.

La Traducción es un mecanismo similar a nat, en donde se modifica la cabecera IPv4 a una IPv6. Uno de los mecanismos más conocido es NAT-PT, sin embargo, no es uno de los más recomendados.

Túneles: Para los casos en los cuales el proveedor de servicios no dispone de soporte IPv6, se utiliza este mecanismo para que el paquete IPv6 pueda atravesar una red que sólo es IPv4. EL túnel encapsula el paquete IPv6 dentro de un paquete IPv4 para que pueda viajar por las redes IPv4. El paquete es desencapsulado al llegar al destino, que debe ser un nodo IPv6 o dual stack.

Sistema de Variables

Según Hernández, R. y otros (2003), una variable “es una propiedad que

puede cambiar y cuya variación es susceptible de medirse u observarse" (p.143). En este sentido, las variables se definen conceptual y operacionalmente.

Conceptualización de Variables

Variable Dependiente: Implementación del Protocolo IPv6.

Variable Independiente: Infraestructura de red de Dato de la UCLA.

Definición Operacional de las variables

Definición Operacional de la Variable Dependiente: Consiste en ejecutar cambios y configuraciones a nivel de software y evaluar el soporte del hardware considerando el proveedor de Servicio de Internet, el hardware y el software.

Definición Operacional de la Variable Independiente: Consiste en determinar elementos que forman la Infraestructura y sus características en relación a la red de dato de la UCLA.

La Operacionalización de las variables Dependiente e Independiente se describe en los Cuadros 1 y 2 respectivamente y son mostrados a continuación.

Cuadro 1

Operacionalización de la Variable Dependiente

Variable	Dimensión	Indicadores	Ítems
Implementación del Protocolo IPv6	Hardware	Conectividad física	Estado de la conectividad física en los equipos de comunicaciones
		Equipos para pruebas	Capacidad de hardware de los equipos que servirán de pruebas
		Equipos en producción	Capacidad de hardware de los equipos de la red en producción

Cuadro 1 Continuación

Variable	Dimensión	Indicadores	Ítems
Implementación del Protocolo IPv6	Software	Funcionalidad del Sistema Operativo	Soporte del protocolo IPv6 en los sistemas operativos de los equipos que intervienen en la Implementación
		Funcionalidad del Sistema Operativo	Estado de configuración del protocolo IPv6
		Requerimiento de Actualización de Sistema Operativo	Efectuar actualizaciones de sistemas operativos en los elementos que forman parte de la Implementación
		Funcionalidad de servicios	Soporte del protocolo IPv6 a nivel de los servicios DNS, DHCPv6, Web en los equipos que intervienen en la implementación
		Requerimiento de actualización de servicios	Actualizar servicios de red (incluidos en la implementación) a versiones con soporte para IPv6
		Normas de comunicaciones	Existencia de un número de sistema autónomo para la UCLA

Cuadro 1 Continuación

Variable	Dimensión	Indicadores	Ítems
Implementación del Protocolo IPv6	Proveedor de Servicios de Internet	Software	Soporte de protocolo de enrutamiento dinámico
		Soporte técnico	Capacidad de respuesta del proveedor de servicio de Internet en configuraciones conjuntas
		Hardware	Conectividad de última milla

Cuadro 2

Operacionalización de la Variable Independiente

Variable	Dimensión	Indicadores	Items
Infraestructura de la red de dato de la UCLA	Enrutadores	Componentes, módulos, tarjetas	Tarjetas, componentes y módulos presentes
	Firewalls	Modelo de equipo	Número de parte
	Conmutadores	Modelo de equipo Funciones adicionales	Número de parte

Autor (2011)

CAPITULO III

MARCO METODOLOGICO

Naturaleza de la Investigación

De acuerdo con el Manual para la Elaboración del Trabajo Conducente a Grado Académico de Especialización, Maestría y Doctorado de la UCLA (2002) donde dice que "el proyecto factible formula propuestas de acción y/o modelo operativos como alternativas de solución al problema planteado", el trabajo "Implementación del protocolo IPv6 en la infraestructura de red de la UCLA" se ubica dentro de la modalidad de proyecto factible apoyado en la investigación de campo y monográfica documental.

Fases del Estudio

A continuación se describen las tres fases fundamentales para la formulación de un proyecto factible que se siguieron en el presente trabajo de grado: Fase I de Diagnóstico, Fase II de Factibilidad y Fase III de Propuesta del Estudio.

Fase I: Diagnóstico

En esta fase se realizó un análisis general de la situación actual del protocolo de nueva generación (IPv6) en relación a la red de dato de la UCLA, aplicando una observación estructurada a los principales elementos de comunicaciones y servicios de la red de dato de la UCLA con la finalidad de determinar el estado de implementación del protocolo IPv6 en la infraestructura de red y su factibilidad de ejecución.

Técnicas e Instrumentos de Recolección de Datos

Para obtener la información necesaria se utilizaron como técnicas la observación estructurada y la revisión documental, estos instrumentos permitieron recolectar los aspectos más importantes acerca del estado administrativo y técnico del protocolo de Internet de nueva generación en la infraestructura de red de dato de la UCLA.

El instrumento se elaboró a través de una tabla de operacionalización de variables, en donde se conceptualizaron y se operacionalilzaron las variables Dependiente e Independiente hasta elaborar los ítems que conforman el instrumento.

Validez del instrumento

Según Balestrini, M. (1998) la validez es un concepto del cual pueden tenerse diferentes tipos de evidencias relacionadas con el contenido, con el criterio y con el constructo. La validez de constructo se refiere al grado en que una medición se relaciona consistentemente con otras, de acuerdo con las hipótesis derivadas teóricamente sobre esa variable.

Para determinar la validez del instrumento se utilizó la técnica del juicio de expertos, eligiéndose especialistas con suficientes conocimientos del área de redes, Telecomunicaciones y metodología de la investigación, quienes presentaron sus recomendaciones en la ejecución del mismo:

- Ing. Msc. Jean Paul Angeli (Docente de la Maestría Cs de la Computación de la UCLA)
- Ads. Junior Escalona (Jefe del Dpto de Redes de Dato de la UCLA)
- Lic. Msc. Virginia Torres (Docente de la asignatura Metodología de la Investigación en la Maestría Cs. De la Computación de la UCLA)

Procedimiento de la Investigación

El procedimiento de la investigación enumera los pasos seguidos para lograr los objetivos de la investigación.

Para alcanzar el objetivo "Diagnosticar la situación actual de la infraestructura de redes de dato de la UCLA en relación a la implementación del protocolo IPv6", se siguieron los siguientes procedimientos:

- Conceptualización de las variables mediante la Operacionalización de las variables
- Medición de las variables de estudio a través de la tabla de Operacionalización de las variables
- Elaboración de un formato de observación de variables (Anexo1).
- Aplicación del formato de observación en los equipos de infraestructura de la red de datos de la UCLA que participaron en los procesos de implementación del protocolo IPv6.

Conclusiones del Diagnóstico

Una vez aplicados los instrumentos descritos anteriormente, se realizó un análisis de los resultaos obtenidos explicándose a continuación:

- La conectividad física en las distintas interfaces de los equipos de telecomunicaciones de la UCLA hacia el proveedor de servicios se encuentran totalmente activas, facilitando así las configuraciones requeridas a nivel de protocolo.
- La interfaces de conexión entre enrutadores internos de la Red de la UCLA están habilitadas y funcionando, permitiendo las configuraciones de enrutamiento que sean necesarias.
- Las conexiones troncales entre los distintos equipos de comunicaciones a nivel de núcleo, distribución y acceso de la red UCLA están funcionando

adecuadamente permitiendo la posibilidad de ejecutar pruebas en cada nivel de la red donde haga falta.

- Se dispone de equipos servidores y estaciones para pruebas con capacidad de hardware, software y conectividad necesarios para simular ambientes equivalentes a la red UCLA y su posterior implementación en la red en producción.
- Los equipos servidores que están en producción en la red UCLA disponen de suficiente capacidad de hardware para soportar posibles actualizaciones de sistema operativo en caso de ser requerido en la implementación.
- El sistema operativo de los equipos de seguridad de la red UCLA (Firewalls) no cuenta con soporte para el protocolo IPv6, haciéndose necesario el cambio de versión a una más nueva.
- Los Routers de borde de la red UCLA poseen instalada una versión del sistema operativo que cuenta con capacidad de utilizar el protocolo IPv6 permitiendo ejecutar las labores de implementación sin necesidad de actualizar a una versión más nueva, evitando la inversión de tiempo en verificaciones asociadas a una nueva versión del mismo.
- La topología de red de la UCLA no requiere el uso de equipos de conmutación con capacidad de nivel de capa de red, siendo transparente a nivel de capa dos y concluyéndose innecesaria la migración de los sistemas operativos de tales equipos.
- Para el sistema operativo Centos 5.5, kernel 2.6.18, no se requiere la actualización de la versión ya que el mismo dispone de los módulos necesarios para el protocolo IPv6, facilitando la inclusión de servicios que lo utilicen.
- Windows XP posee soporte limitado para el protocolo IPv6, ya que permite su habilitación y funciona con direccionamiento estático pero carece de un cliente DHCPv6, siendo necesario instalar un cliente DHCPv6 externo o migrar a la versión Windows 7.

- Windows 7 posee soporte para el protocolo IPv6 incluyendo el cliente DHCPv6, siendo innecesario la instalación de clientes adicionales en este sistema operativo.
- La actual versión de BIND (versión 9) en los servidores DNS cuenta con soporte para IPv6, permitiendo la transición ejecutando las configuraciones requeridas sin cambio de versión.
- El servicio DHCPv6 dispone de soporte operacional para el sistema operativo Windows 2008, siendo este último el escogido para la Implementación.
- Para el servicio Web se dispone de IIS 6 y Apache 2.2, ambas con soporte para el protocolo IPv6, permitiendo ejecutar las configuraciones necesarias para el inicio del servicio en los equipos incluidos en la implementación.

Para el objetivo "Determinar la factibilidad operativa, técnica, y económica para la implementación del protocolo IPv6 en la infraestructura de red de dato de la UCLA" se observaron y analizaron los factores técnicos, costos de operación y recursos disponibles con la finalidad de establecer los criterios que llevan al conocimiento del sistema y su viabilidad de ejecución.

Fase II: Factibilidad

El estudio del entorno en el que se desarrolló la Implementación del Protocolo IPv6, determinó la factibilidad del objetivo propuesto, garantizando la aceptación del mismo.

Factibilidad Técnica

Mediante un análisis del hardware y software con capacidad de soporte del protocolo IPv6 en los elementos que integran la infraestructura de redes de dato de la UCLA así como la consideración de la experticia y capacidad técnica del personal

integrante del Departamento de Redes de Dato, se verificó el cumplimiento de estos parámetros para esta fase de la investigación.

Factibilidad Operativa

La posibilidad de acceso a los recursos tecnológicos que conforman la infraestructura de redes de dato de la UCLA, los equipos servidores, estaciones de prueba y en producción, permitió ejecutar, de forma controlada, las configuraciones, actualizaciones y demás procesos requeridos para desarrollar el presente proyecto sin inconvenientes de tipo administrativo.

Factibilidad Económica

Para considerar la factibilidad económica se tomaron en cuenta algunos factores conducentes a comprobar su aceptación: los equipos de comunicaciones como routers, firewalls y equipos de conmutación en el núcleo de la red (core) disponen de los elementos de hardware necesarios para el soporte del protocolo IPv6 sin requerir ninguna adquisición de módulos o tarjetas adicionales, así mismo, para los servicios principales de la red, se dispone de servidores con capacidad de hardware y software para la implementación de IPv6. En el caso de los sistemas operativos tanto de los equipos de enrutamiento, seguridad, conmutación, servidores y estaciones de trabajo, se dispone para la fecha de posibilidad de actualización o descarga de versiones actualizadas sin costo, siendo una ventaja para el hardware con capacidad para IPv6 con versiones nuevas del software.

Una vez descritas las fases del estudio, se determinó justificada la elaboración de un proyecto factible apoyado en la investigación de campo que permitió la solución de la problemática planteada con los beneficios que brinda el mismo a la red de Datos de la UCLA enmarcado en el avance de tecnológico hacia Internet de próxima generación específicamente para el proyecto Reacciun2.

CAPITULO IV

PROPUESTA DEL ESTUDIO

Los resultados logrados producto de los instrumentos aplicados en la investigación permitieron diagnosticar y conocer el estado de los elementos que constituyen la infraestructura de red de datos de la UCLA y sus principales servicios en relación al protocolo IPv6. Se presenta a continuación la propuesta de diseño de implementación del protocolo IPv6 en la infraestructura de red de dato de la UCLA.

Descripción de la Propuesta

Para el diseño de la Implementación del Protocolo IPv6 en la Infraestructura de red de dato de la UCLA se tomó como base el documento de planificación para implementación de IPv6 de la empresa Sun Microsystem ya que resume de forma precisa y detallada todos los procesos necesarios a tomar en cuenta para la puesta en marcha del protocolo en una red de datos.

Desarrollo de la Propuesta

Se describen a continuación los pasos seguidos en la implementación del protocolo IPv6:

1) Preparar el hardware para admitir IPv6.
2) Disponer de un ISP que admita IPv6
3) Disponer de un prefijo de sitio
4) Seleccionar el mecanismo de transición
5) Crear un plan de direccionamiento de subredes

6) Crear un plan de direcciones par entidades de la red
7) Desarrollar directrices de seguridad de IPv6
8) Configurar DMZ's
9) Habilitar nodos para que admitan IPv6
10) Activar servicios de red.

Preparar el hardware para admitir IPv6

La preparación de la topología de la red para admitir el protocolo IPv6 consiste en comprobar que el hardware incluido en la implementación, soporta el protocolo o se puede actualizar para tal fin. Para el caso de la red de la UCLA, se comprobó mediante la ejecución de los comandos necesarios y la consulta a la documentación del fabricante, que los módulos de los routers cuentan con las características necesarias para configurar IPv6. Dada la topología de la red UCLA, los conmutadores a nivel de acceso, distribución y núcleo (core), no requieren capacidad para funcionamiento en capa de red (capa3), siendo transparente a nivel de la capa de enlace de datos (capa 2), permitiendo la transición a IPv6 sin efectuar modificaciones de la topología.

Disponer de un ISP que admita IPv6

La red de la UCLA, como integrante del proyecto REACCIUN2, posee conectividad con el Centro Nacional de Innovación Tecnológica (CENIT) como proveedor de servicios de Internet (ISP). Este organismo se encarga de centralizar las operaciones técnicas de comunicaciones de la red Académica Nacional y cuenta con la infraestructura necesaria para utilizar el protocolo IPv6.

Disponer de un prefijo de sitio

El Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC) asignó un bloque de direcciones IPv6 /32 a la UCLA tal como se indica en el sitio lacnic.net, disponiendo de esta manera de uno de los requisitos para implementar el protocolo en la infraestructura de red.

Seleccionar un método de transición a IPv6

La capacidad Dual Stack del proveedor de servicios CENIT, el prefijo IPv6 asignado por LACNIC a la UCLA, la capacidad de soporte del protocolo en los principales equipos de infraestructura de la red y servidores, la topología existente conmutada en su totalidad con segmentos y redes locales virtuales (VLAN's) con direccionamiento IPv4; fueron los factores considerados para la escogencia del mecanismo Doble Pila (Dual Stack) como método de transición para la infraestructura de red de dato de la UCLA. En la Figura 13 se observa la topología de la Red UCLA con los equipos que formaron parte de la Implementación de IPv6.

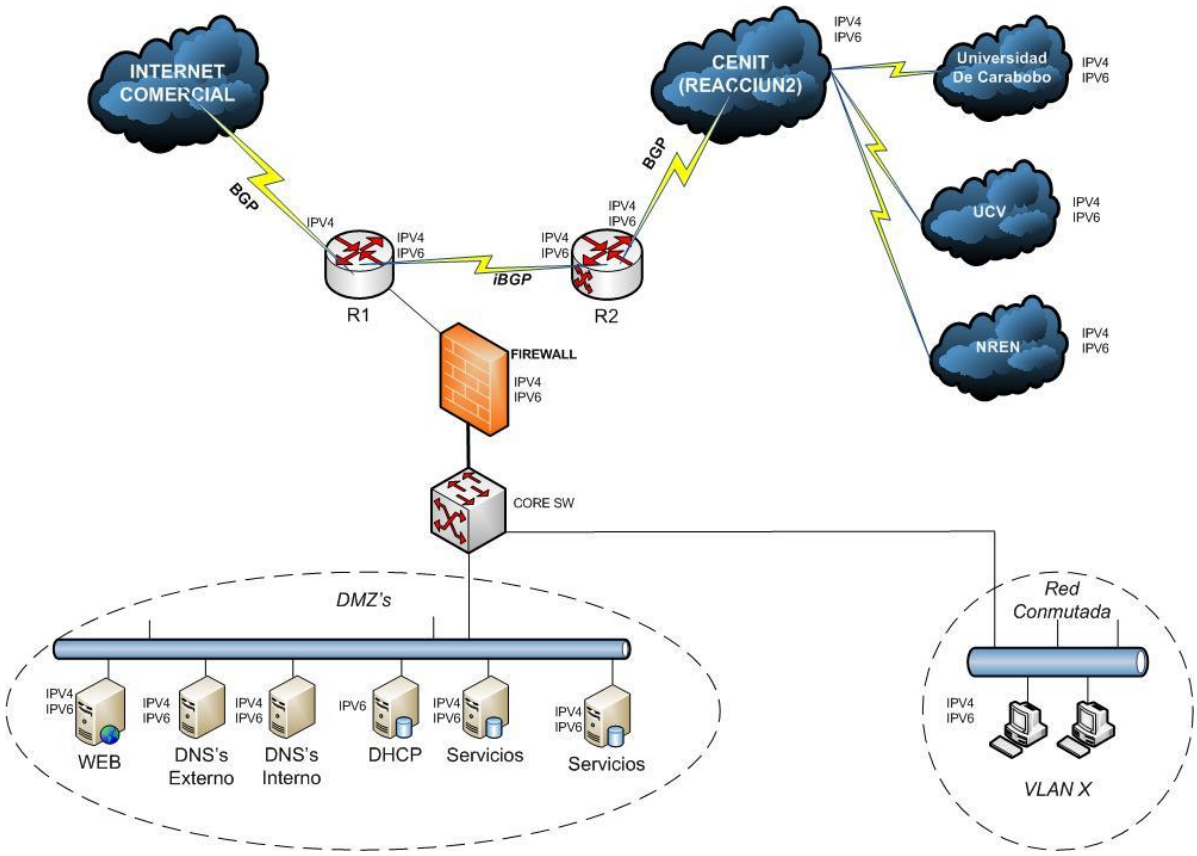

Figura 13:Topología Backbone de la Red UCLA. **Fuente:** Autor (2011)

Crear un Plan de direcciones en subredes

El plan de direccionamiento en subredes consiste en planificar en la topología el esquema de direcciones IPv6 a configurar en los distintos segmentos de la red UCLA, tomando en cuenta la situación del protocolo IPv4 en relación al direccionamiento en subredes y el bloque de direcciones IPv6 asignadas por LACNIC. Tomando como base el esquema de direccionamiento en subredes existente para IPv4, se inició asignando los segmentos de red correspondientes a las interfaces Loopback, luego la asignación correspondiente a equipos de infraestructura (Routers) continuando con los segmentos para servidores en las diferentes DMZ's concluyendo con los segmentos adecuados para los equipos de usuarios finales. Se muestra en el cuadro 3 la tabla de segmentación de redes en IPv6 para la UCLA.

Cuadro 3

Plan de direccionamiento en subredes

Segmentos	**Descripción**
X800:x000:FFFF::/64	Subred Para Loopbacks
X800:x000:FFFF:1::/64	Subred Para Infraestructura
X800:x000:FFFD::/64	Subred Para Infraestructura
X800:x000:1:1x1::/64	DMZ1
X800:x000:1:1x2::/64	DMZ2
X800:x000:1:1y2::/64	DMZ0
X800:x000:1:1x0::/64	Direccionamiento Red Reacciun
X800:x000:1:0::/64	Subred de Videoconferencia
X800:x000:1:2x2::/64	Subred para equipos de usuarios finales en el segmento 2x2 (Vlan 2x2)

Fuente: Autor (2011)

Crear un plan de direcciones para entidades de la red

Una vez desarrollado el direccionamiento IPv6 de subredes para cada segmento de la red UCLA, se procedió a crear una planificación direcciones para los equipos que intervinieron en la Implementación: Routers (Interfaces físicas e interfaces Loopbacks), Firewalls (Interfaces, DMZ's, VLAN's), Servidores y estaciones de trabajo. Esta planificación se describe en el Cuadro 4

Cuadro 4

Plan de direcciones para entidades de la red

Segmentos	**Descripción**
X800:x000:FFFF::2/64	Loopback Router 2
X800:x000:FFFF::1/64	Loopback Router 1
x800:z0:FFFF:19::3/64	Router 2 Asignada por proveedor para BGP

Cuadro 4. Continuación

Segmentos	Descripción
x800:x000:1::1/64	Router 2 Interfaz en subred para Videoconferencia
x800:x000:FFFF:1::2/64	Router 2, iBGP
x800:x000:FFFF:1::1/64	Router 1, iBGP
x800:x000:1:1x0::1/64	Router 1, Subred Reacciun 1
X800:x000:FFFD::2/64	Router 1, Inerconexion con Firewall
X800:x000:FFFD::1/64	Firewall, Interconexión con Router 1
X800:x000:1:1x2::2/64	DNS LAN 1 (DMZ 0)
X800:x000:1:1x2::3/64	DNS LAN 2 (DMZ 0)
X800:x000:1:1x2::68/64	DHCPv6
X800:x000:1:1x0::2/64	DNS Externo1
X800:x000:1:1x0::4/64	DNS Externo2
X800:x000:1:1x2::74/64	Ftp intranet
X800:x000:1:1x2:77/64	Correo Intranet (Servicio en período de prueba)
X800:x000:1:1x1::11/64	Web UCLA
X800:x000:1:1x1::14/64	Postgrado
X800:x000:1:1x1::17/64	Cofeu
X800:x000:1:1x1::248/64	Servidor de prueba de servicios
X800:x000:1:1x2::60/64	Seducla
X800:x000:1:1x2::63/64	Biblioteca Virtual
X800:x000:1:2x2::20-X800:x000:1:2x2::40/64	Rango de direcciones IPv6 en un ámbito del servidor DHCPv6

Autor (2011)

Desarrollar directrices de seguridad de IPv6

De forma equivalente a la administración de seguridad de la red UCLA para el

protocolo IPv4 en todos sus servicios, se planificó el esquema de seguridad a seguir para los equipos que integran la implementación del protocolo IPv6. En el caso de los servidores con sistema operativo Linux, posterior a la habilitación del protocolo IPv6 se procedió a la configuración del firewall ip6tables, permitiendo únicamente aquellos servicios considerados como admitidos tanto de entrada como de salida de acuerdo a las características ofrecidas por cada uno en la red. En el equipo firewall de seguridad perimetral se construyeron las políticas necesarias para permitir el acceso a los servicios publicados tanto en la Intranet como hacia el exterior especificando la permisología de origen y destino de forma similar a las configuraciones existentes para IPv4.

Configurar DMZ`s

Las zonas desmilitarizadas o DMZ's consisten en subredes lógicas o físicas que contienen servicios que se exponen a redes no confiables, como Internet. La topología de red de la UCLA en IPv4 cuenta con Zonas DMZ con la finalidad de agregar una capa adicional de seguridad para los servicios necesariamente expuestos por naturaleza, por ejemplo: servicios web, ftp, bibliotecas, educación a distancia, correo electrónico, información de postgrado, repositorio, etc. El mecanismo Doble Pila (Dual Stak) se implementó en cada una de estas zonas para permitir el despliegue IPv6 en los servidores que fuera necesario. Cada DMZ corresponde a un segmento de red en la topología y debido a que se seleccionó Dual Stack, cada segmento se configuró en el equipo de seguridad Firewall con una subred IPv6 de acuerdo al plan de direccionamiento de segmentos de red.

Habilitar nodos para que admitan IPv6

Una vez comprobados los requisitos necesarios para habilitar IPv6 en Routers, Firewalls, servidores y estaciones, se procedió a la configuración del protocolo en cada uno de los equipos nombrados.

Routers: La configuración del protocolo IPv6 se inició con el router de borde con acceso a la red Reaccuin 2, denominado Router 2. Posteriormente se configuró el Router 1. Se presentan a continuación los pasos seguidos en dicha tarea:

- Habilitar el reenvío de paquetes IPv6 : comando Router2(config)# **ipv6 unicast-routing**
- Configurar dirección IPv6 (asignada por el proveedor) en interfaz ATM:

  interface ATM1/0.x6 point-to-point

  ipv6 address x800:x0:FFFF:19::3/64
- Verificar respuesta ping al proveedor de servicio (ISP)

  ROUTER2#ping x800:x0:ffff:19::1

  Type escape sequence to abort.

  Sending 5, 100-byte ICMP Echos to x800:x0:FFFF:19::1, timeout is 2 seconds:

  !!!!!

  Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms

- Configurar dirección IPv6 en las interfaces Loopback e iBGP

  interface Loopback0

  ipv6 address x800:x000:FFFF::x/64

  interface GigabitEthernet 0/x

  description Enlace iBGP Router1 - Router2

  ipv6 address x800:x000:FFFF:x::x/64

- Configurar interfaces Loopback, de conexión con firewall y de conexión con Router 2 para iBGP en Router1.

  Habilitar el reenvío de paquetes IPv6 , comando: Router1(config)# **ipv6 unicast-routing**
  Configurar las interfaces Loopback y Gigabit
  interface Loopback0

  ipv6 address x800:x000:FFFF::1/64

  interface GigabitEthernet1/2

  description Enlace Router2-Firewall

ipv6 address x800:x000:FFFD::2/64

interface GigabitEthernet5/2

description Enlace iBGP Router1 - Router2

ipv6 address x800:x000:FFFF:1::1/64

ROUTER1#ping x800:x000:FFFF:1::2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to x800:x000:FFFF:1::2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms

ROUTER1#

ROUTER1#PING 2800:A000:FFFF::2

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 2800:A000:FFFF::2, timeout is 2 seconds:

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 0/0/4 ms

ROUTER1#

- Agregar parámetros IPv6 en las configuraciones BGP de ROUTER1

  Establecer sesión BGP

  neighbor x800:x0:FFFF:19::1 remote-as 27807

  neighbor x800:30:FFFF:19::1 description REACCIUN2-C3

  neighbor x800:30:FFFF:19::1 password 7 1

  neighbor x800:x0:FFFF:19::1 remote-as 27686

  neighbor x800:A000:FFFF::1 description IBGP-IPV6-7600-7200

  neighbor x800:A000:FFFF::1 password 7 1

  neighbor x800:A000:FFFF::1 update-source Loopback0

  address-family ipv6

  network x800:x000::/32

- Agregar parámetros IPv6 en las configuraciones BGP de ROUTER2

  neighbor x800:x000:FFFF::2 remote-as x7x8x

neighbor x800:x000:FFFF::2 description IBGP-Ipv6_7600_7200

neighbor x800:x000:FFFF::2 password 7 1

neighbor x800:x000:FFFF::2 update-source Loopback32

address-family ipv6

network x800:x000::/32

- Verificar que la sesión BGP se encuentra funcionando

ROUTER1#sh bgp ipv6 unicast summary

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

x800:30:FFFF:19::1

4 27807 11572764 788776 10659202 0 0 5d23h 5294

x800:30:FFFF:19::2

4 27807 0 0 0 0 0 never Active

x800:x000:FFFF::1

4 27686 790231 9305729 10659202 0 0 7w0d 8

ROUTER2#sh bgp ipv6 unicast summary

Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd

x800:x000:FxFF::2

4 27686 7254092 71547 9902037 0 0 7w0d 5300

- Configurar rutas estáticas en ROUTER2 de acuerdo al plan de direccionamiento de las DMZ's y subredes incluidas en la implementación.

ipv6 route x800:x000:1:151::/64 x800:x000:FFFD::1

ipv6 route x800:x000:1:152::/64 x800:x000:FFFD::1

ipv6 route x800:x000:1:172::/64 x800:x000:FFFD::1

ipv6 route x800:x000:FFFF::2/128 x800:x000:FFFF:1::2

Firewall:

- Configurar dirección IPv6 en la interfaz de conectividad Firewall-Router2

x800:x000:FxxD::1/64

- Crear una ruta por defecto para el protocolo IPv6 configurando como próximo salto la dirección IPv6 del Router directamente conectado al firewall

  Destino ::/0 (cualquier destino)

  Puerta de enlace x800:x000:fxfd::2 (Dirección IPv6 del Router)

- Configurar direcciones IPv6 de las Zonas DMZ's en las interfaces del equipo de seguridad Firewall para permitir el InterVLAN Routing:

  DMZ0 x800:x000:1:1x2::1/64

  DMZ1 x800:a000:1:1x1::1/64

  DMZ2 x800:a000:1:1x2::1/64

  VLANx x800:a000:1:x::1/64

- Configurar el Intervlan Routing para cada segmento de red de la Implementación IPv6:

  DMZ0 → DMZ1

  DMZ0 → DMZ2

  DMZ0 →Red LAN (Segmento de prueba)

  DMZ0 → Redes Externas

  DMZ1 → DMZ0

  DMZ1 → DMZ1

  DMZ1 → Red LAN (Segmento de prueba)

  DMZ1 → Redes Externas

  DMZ2 → DMZ0

  DMZ2 → DMZ1

  DMZ2 → RedLAN

  DMZ2 → Redes Externas

  Red LAN(Segmento de prueba) → DMZ0

  Red LAN(Segmento de prueba) → DMZ1

  Red LAN (Segmento de prueba)→ DMZ2

  Red LAN (Segmento de prueba)→ Redes Externas

Redes Externas → DMZ0

Redes Externas → DMZ1

Redes Externas → DMZ2

Redes Externas → Red LAN (Segmento de prueba)

- Configurar en el Firewall las políticas de seguridad requeridas de acuerdo a los servicios a ser permitidos en cada segmento de red y equipos tal como ilustra el Cuadro 5:

Cuadro 5

Políticas de seguridad IPv6 en Firewall

Destino	**Origen**	**Servicio**	**Tr. Shape**	**Acción**
DNS LAN1,2 (DMZ 0)	DMZ 1,2 Segmento LAN Internet	DNS, Ping6 DNS, Ping6 Ping6	-	Permitir
DMZ 1,2 Segmento LAN Internet	DNS LAN1,2 (DMZ 0)	HTTP, Ping6 DNS HTTP, Ping6		
DHCPv6 (Segmento LAN X)	DMZ 0,1,2 Internet	DNS, Ping6 DNS, Ping6 Ping6	-	Permitir
DMZ 0,1,2 Internet	DHCPv6 (Segmento LAN)	Ping6, DNS Ping6, HTTP, HTTPS	-	Permitir
Ftp intranet	DMZ 0,1 Segmento LAN Internet	HTTP, FTP,Ping6 HTTP,Ping6 HTTP, Ping6	256K	Permitir

Cuadro 5. Continuación

Destino	Origen	Servicio	Tr. Shape	Acción
DMZ 0,1 Segmento LAN Internet	Ftp intranet	DNS,HTTP,HTTPS, Ping6 FTP, Ping6 FTP, Ping6, HTTP		Permitir
Correo Intranet	DMZ 0,1 Segmento LAN Internet	HTTP,HTTPS, SMTP, Ping6 HTTP,HTTPS, SMTP, Ping6 HTTP,HTTPS, Ping6		Permitir
DMZ 0,1 Segmento LAN Internet	Correo Intranet	DNS,HTTP, HTTPS, SMTP, Ping6 Ping6 DNS,HTTP, HTTPS, Ping6		Permitir
Web UCLA, Postgrado, Cofeu	DMZ 0,2 Segmento LAN Internet	HTTP, Ping6 HTTP HTTP, Ping6		Permitir
DMZ 0,2 Segmento LAN Internet	Web UCLA, Postgrado, Cofeu	DNS,HTTP, HTTPS Ping6 Ping6 HTTP, HTTPS Ping6		Permitir

Cuadro 5. Continuación

Destino	Origen	Servicio	Tr. Shape	Acción
Seducla, Biblioteca Virtual	DMZ 0,2 Segmento LAN Internet	HTTP, Ping6 HTTP HTTP, Ping6		Permitir
DMZ 0,2 Segmento LAN Internet	Seducla, Biblioteca Virtual	DNS,HTTP, HTTPS Ping6 Ping6 HTTP, HTTPS Ping6		Permitir
Servidor de prueba	DMZ 0,1 Segmento LAN Internet	HTTP, Ping6 HTTP HTTP, Ping6		Permitir
DMZ0,1 Segmento LAN Internet	Servidor de prueba	DNS,HTTP, HTTPS Ping6 Any		Permitir
Segmento LAN	DMZ 0,1,2	DNS, Ping6		Permitir
DMZ 0,1,2 Internet	Segmento LAN	DNS, HTTP, Ping6 HTTP, HTTPS, Ping6		Permitir

Autor (2011)

- Ejecutar pruebas de conectividad a cada segmento DMZ desde el Router con conexión al CENIT (ROUTER 1), en la figura 14 se muestra el resultado:

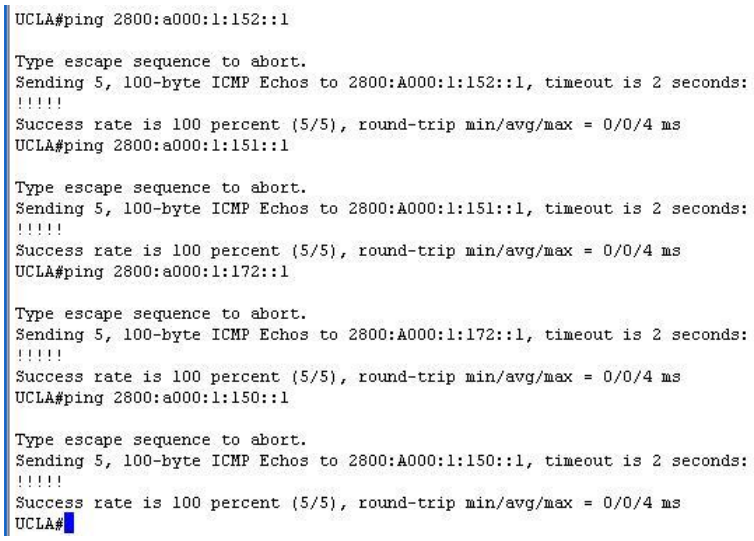

Figura 14: Pruebas de conectividad Intervlan**. Fuente**: Autor (2011)

- Ejecutar pruebas de conectividad IPv6 hacia el proveedor CENIT desde Router 2. En la figura 15 se muestra el resultado del traceroute al CENIT.

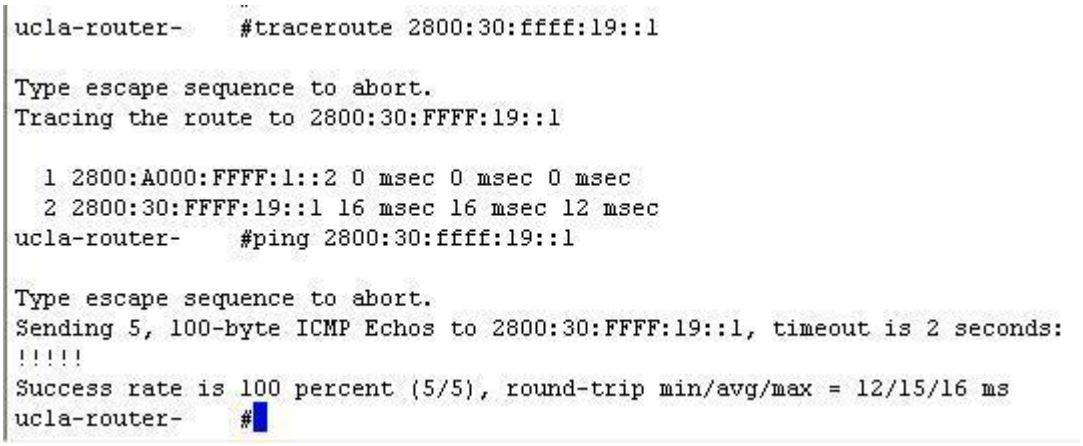

Figura 15: Pruebas de conectividad con proveedor**. Fuente:** Autor 2011

Servidores:

- Configurar el protocolo IPv6 en los equipos incluidos en la Implementación listados en el Cuadro 4.

Para cada sistema operativo se ejecutaron distintos comandos relacionados con la instalación, habilitación y configuración del protocolo, se muestra a continuación el proceso general, quedando entendido que cada equipo con igual sistema operativo se

configuró de la misma manera con la dirección IPv6 que le correspondió. El cuadro 6 ilustra la ejecución de comandos para configuración de Pv6.

Cuadro 6

Configuración del Protocolo IPv6

Sistema Operativo	**Explicación**
Centos 5.5	/etc/sysconfig/network NETWORKING_IPV6=yes /etc/sysconfig/network-scripts/ifcfg-eth0 IPV6ADDR=x800:x000:1:152::248 IPV6_DEFAULTGW=xx00:xx00:x:xxx::x IPV6INIT=yes /etc/resolv.conf Direcciones IPv4 o IPv6 de los servidores DNS
Windows XP, Windows 2003 Server, Windows 2008 Server	C:\> netsh interface ipv6 install C:\> netsh interface ipv6 add address "Nombre de la nic" **Dirección ipv6** netsh interface ipv6 add route ::/0 "Nombre de la nic" **Puerta de enlace** netsh interface ipv6 reset C:\> netsh interface ipv6 **add dns** " Nombre de la nic " **FEC0:0:0:FFFF::1**

Fuente: Autor (2011)

- Ejecutar pruebas de conectividad entre cada segmento de red (Intervlan Routing). La figura 16 muestra la conectividad entre DMZ`s.

  Origen DMZ0, destino DMZ2

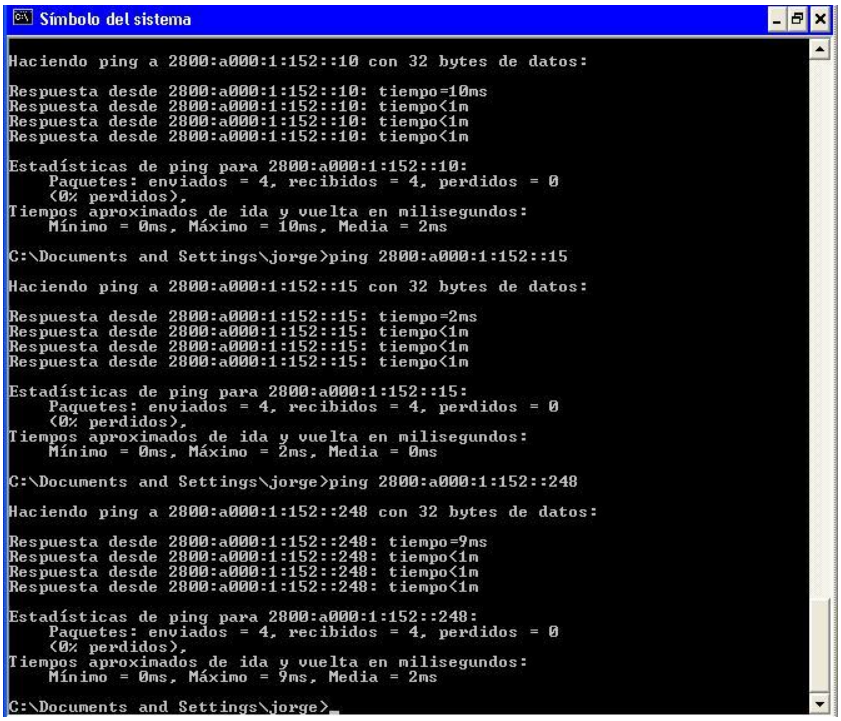

Figura 16: Pruebas de conectividad entre DMZ's**. Fuente:** Autor (2011)**.**

La figura 17 muestra las pruebas de conectividad entre DMZ 0 y DMZ1.

Origen DMZ0, destino DMZ1

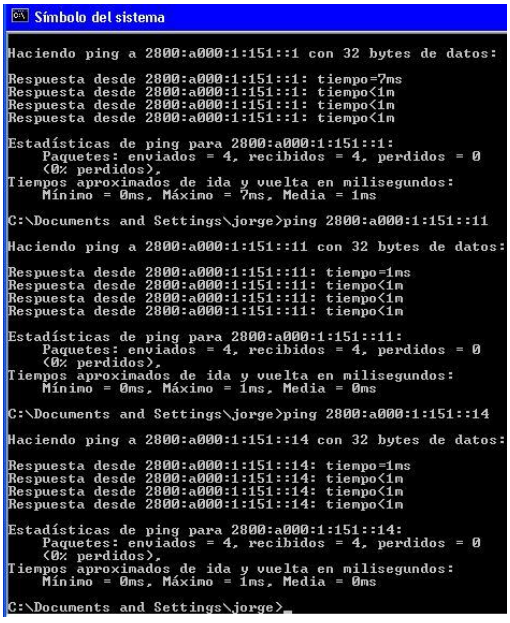

Figura 17: Pruebas de conectividad entre DMZ's**. Fuente:** Autor (2011)**.**

La figura 18 muestra las pruebas de conectividad entre DMZ2, DMZ0 y DMZ1.

Origen DMZ2, destino DMZ0 y DMZ1

```
PING 2800:a000:1:172::101(2800:a000:1:172::101) 56 data bytes
64 bytes from 2800:a000:1:172::101: icmp_seq=0 ttl=127 time=3.81 ms
64 bytes from 2800:a000:1:172::101: icmp_seq=1 ttl=127 time=0.593 ms
64 bytes from 2800:a000:1:172::101: icmp_seq=2 ttl=127 time=0.659 ms
64 bytes from 2800:a000:1:172::101: icmp_seq=3 ttl=127 time=0.753 ms

--- 2800:a000:1:172::101 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3053ms
rtt min/avg/max/mdev = 0.593/1.455/3.817/1.365 ms, pipe 2
[root@palavecino etc]# ping6 2800:a000:1:151::11
PING 2800:a000:1:151::11(2800:a000:1:151::11) 56 data bytes
64 bytes from 2800:a000:1:151::11: icmp_seq=0 ttl=63 time=5.99 ms
64 bytes from 2800:a000:1:151::11: icmp_seq=1 ttl=63 time=0.740 ms
64 bytes from 2800:a000:1:151::11: icmp_seq=2 ttl=63 time=0.641 ms

--- 2800:a000:1:151::11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2037ms
rtt min/avg/max/mdev = 0.641/2.457/5.992/2.500 ms, pipe 2
[root@palavecino etc]# ping6 2800:a000:1:151::14
PING 2800:a000:1:151::14(2800:a000:1:151::14) 56 data bytes
64 bytes from 2800:a000:1:151::14: icmp_seq=0 ttl=63 time=1.32 ms
64 bytes from 2800:a000:1:151::14: icmp_seq=1 ttl=63 time=0.768 ms
64 bytes from 2800:a000:1:151::14: icmp_seq=2 ttl=63 time=0.749 ms
64 bytes from 2800:a000:1:151::14: icmp_seq=3 ttl=63 time=0.771 ms

--- 2800:a000:1:151::14 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3055ms
rtt min/avg/max/mdev = 0.749/0.902/1.320/0.241 ms, pipe 2
[root@palavecino etc]#
```

Figura 18: Pruebas de conectividad entre DMZ's**. Fuente:** Autor (2011)**.**

Activar Servicios de Red

Una vez comprobado el soporte del protocolo IPv6 en los servicios más importantes de la Red UCLA, se procedió a configurarlos en los servidores correspondientes.

Servicio de Nombres de Dominio (DNS)

Dado que ya se disponía de una versión de servicio de nombre de dominio (BIND 9.3.6) con soporte para IPv6, se trabajó en tal aplicación agregando los

parámetros requeridos para habilitar el funcionamiento del nuevo protocolo.

Para los servidores de nombre de dominio primarios se configuró el archivo /etc/named.conf añadiéndose la directiva listen-on-v6{any;}; y modificando las acl para permitir el segmento IPv6 de interés:

```
Archivo named.conf
acl Red _de_Empresa {
        127.0.0.1/32;
        10.0.0.0/8;
        ::1;
        2001:1234::/32;
};
acl dns_secundarios {
     10.0.0.200;
     2001:1234::200;
};
options {
        allow-recursion { Red _de_Empresa;};
        directory “/var/named”;
        listen-on-v6 { any; };
        notify yes;
        allow-notify { dns_secundarios; };
        };
```

En el archivo named.conf se declaró además la zona de resolución inversa correspondiente al prefijo que fue delegado por parte del proveedor de servicios (LACNIC) 2001:1234::/32 (Prefijo de ejemplo). El nombre de dominio usado para la resolución inversa en IPv6 es ip6.arpa.

```
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
 “0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.3.2.1.1.0.0.2.ip6.arpa” {
        type master;
        File “2001_1234.zone”;
        allow-transfer { dns_secundarios; };
}
```

Se agregaron los registros AAAA en la zona de resolución directa, de esta forma, los equipos con dual stack configurado tienen los registros A y AAAA.

Archivo univ.edu.ve

```
$TTL 86400
@       IN              SOA     dns1.univ.edu.ve. dnsadmin.univ.edu.ve. (
                                2002071901 ;    serial
                                28800 ;         refresh
                                7200 ;          retry
                                604800 ;        expire
                                86400 ;         ttk
                        )
                        IN      NS      dns1.univ.edu.ve.
                        IN      NS      dns2.univ.edu.ve.

Serv_Biblioteca         IN      A       10.0.0.3
                        IN      AAAA    2001:1234::3
Serv_medios             IN      A       10.0.0.4
                        IN      AAAA    2001:1234::4
Serv_sin_IPv6           IN      A       10.0.0.5
```

Se crearon los archivos de zona para resolución inversa de direcciones IPv6. Estos contienen únicamente direcciones IPv6.

Archivo 2001_1234.zone

```
$TTL 86400
@       IN              SOA     dns1.univ.edu.ve. dnsadmin.univ.edu.ve. (
                                2002071901 ;    serial
                                28800 ;         refresh
                                7200 ;          retry
                                604800 ;        expire
                                86400 ;         ttk
                        )
                        IN      NS      dns1.univ.edu.ve.
                        IN      NS      dns2.univ.edu.ve.
3.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.3.2.1.1.0.0.2.ip6.arpa.
IN      PTR     Serv_Biblioteca.univ.edu.ve.
4.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.3.2.1.1.0.0.2.ip6.arpa.
IN      PTR     Serv_medios.univ.edu.ve.
```

Para los servidores de nombre de dominio secundarios se siguió el esquema mostrado anteriormente en los servidores DNS primarios con la diferencia de que en el archivo named.conf se indica las zonas de tipo esclavo y la dirección IPv6 del maestro.

```
zone
 “0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.4.3.2.1.1.0.0.2.ip6.arpa” {
        type slave;
        File “2001_1234.zone”;
        masters { 2001:1234::201; };
}
```

Una vez culminada la etapa de configuración de los servidores DNS primarios

y secundarios tanto internos como externos se procedió a ejecutar pruebas de resolución de nombre. Se muestran los resultados a continuación:

Utilizando el comando host

[root@lavecino ~]# host repositorio.ucla.edu.ve
repositorio.ucla.edu.ve has address 72.0.2.3
repositorio.ucla.edu.ve has IPv6 address 800:000:1:12::3

[root@lavecino ~]# host grado.ucla.edu.ve
grado.ucla.edu.ve has address 72.0.1.14
postgrado.ucla.edu.ve has IPv6 address 800:000:1:11::14

Realizando una consulta inversa

[root@lavecino ~]# host 800:000:1:11::14
4.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.5.1.0.1.0.0.0.0.0.0.a.0.0.8.2.ip6.arpa domain name pointer grado.ucla.edu.ve.

Haciendo la consulta al dns secundario utilizando IPv6

[root@palavecino ~]# host -t aaaa grado.ucla.edu.ve 800:a00:1:12::3
Using domain server:
Name: 800:a00:1:12::3
Address: 800:a000:1:12::3#53
Aliases:
grado.ucla.edu.ve has IPv6 address 800:a00:1:11::14

Servicio Web APACHE

Las versiones de Apache desde 2.0.x en adelante poseen el soporte para IPv6 habilitado por defecto, una vez instalado, hay que iniciarlo para que responda por IPv6. El archivo /etc/httpd/conf/httpd.conf controla a través de la directiva "*Listen"* las direcciones IP y los puertos por los que responde el servidor web.

Para habilitar el protocolo se procedió de la siguiente manera:

Agregar la línea IPv6 en el archivo httpd.conf

Listen A.B.C.D:80

Listen [2X00:X000:X:X::X]:80

Reiniciar el servicio Web

service httpd restart

Configurar ip6tables para permitir el acceso al servidor web vía IPv6.

-A RH-Firewall-1-INPUT -m tcp -p tcp --dport 80 -j ACCEPT

Reiniciar el servicio IP6TABLES:

service ip6tables restart

Verificar que Apache está funcionando en modo DualStack

netstat -tulpn | grep :80

tcp 0 0 74.86.48.99:80 0.0.0.0:* LISTEN 4473/httpd

tcp 0 0 2607:f0d0:1002:11::4:80 :::* LISTEN 4473/httpd

Servicio Web IIS

Desde la versión 6, IIS tiene soporte para el protocolo IPv6. Para la configuración de IIS se procedió de la siguiente manera:

Instalación del protocolo IPv6 desde la línea de comando de MS-DOS.

C:\netsh interface ipv6 install

Configuración del protocolo IPv6 de acuerdo a la planificación de direcciones IPv6.

Para los casos en los que un mismo hardware aloje varios sitios Web, se pueden asignar tantas direcciones IPv4 e IPv6 como sitios se encuentren instalados en el servidor. Para el caso específico, se añadieron las direcciones IPv6 correspondientes a cada sitio y se procedió a realizar cambios necesarios en las propiedades de IIS. Los pasos seguidos fueron los siguientes:

Ejecutar Herramientas Administrativas, Administrador de IIS, Clic derecho en el sitio a configurar y continuar de la siguiente forma:

En las propiedades se debe escoger “Ninguna Asignada” como Dirección IP, ir a la

configuración avanzada e indicar el valor del encabezado, que no es otra que el nombre de dominio del servicio que estamos habilitando. Para el resto de los sitios web alojados se procede de la misma manera que la anterior y luego se verifica la conectividad vía IPv6.

Reiniciar el servicio IIS para que comience a responder a las solicitudes IPv6.

Servicio Dynamic Host Control Protocol versión 6 (DHCPv6)

El servicio DHCPv6 se configuró con la finalidad de aumentar la capacidad de respuesta en el soporte para los futuros usuarios del protocolo IPv6.

Se inicio el proceso instalando el servicio, seleccionando el protocolo IPv6 para la configuración DHCP y creando el ámbito de interés. Para la creación de un ámbito nuevo el sistema solicita el prefijo, el intervalo de concesión y la opción de activación del mismo. Una vez creado y habilitado, se comenzaron a observar las concesiones de direcciones IPv6 administradas por el sistema y recibidas por los clientes DHCPv6.

Con la finalidad de mejorar la administración de red, se procedió a exportar en archivos txt todas las concesiones otorgadas por el servidor, archivo en el cual aparecen los parámetros de funcionamiento del cliente DHCPv6 (IAID y el DUID). Para llevar un control de direcciones, se creó una exclusión absoluta del ámbito DHCPv6, es decir, ninguna dirección IPv6 sería otorgada por el servidor, a continuación, con los datos obtenidos en el archivo txt nombrado anteriormente, se realizaron las reservas de aquellos PCs que interesaba que se conectaran a la red. Una vez concluida esta configuración, se obtuvo un mejor control en la distribución de direcciones IPv6 del ámbito.

Publicación de servicios hacia el Exterior

Una vez los servicios se encontraban funcionando en la Intranet, se procedió a realizar las solicitudes de soporte a cada uno de los proveedores relacionados:

CENIT, CONATEL y LACNIC para el anuncio del prefijo IPv6 en BGP, el registro de las direcciones IPv6 para los servidores DNS externos y la delegación inversa de DNS respectivamente.

El anuncio del bloque de UCLA se inició gracias a las gestiones del CENIT a RedCLARA, Tinet, AMPATH, Internet2 e Internet comercial. Los servidores DNS públicos se encontraban registrados con las direcciones IPv4, agregando el registro de las direcciones IPv6 por parte de CONATEL. La figura 19 muestra el resultado del registro del DNS1 de la UCLA.

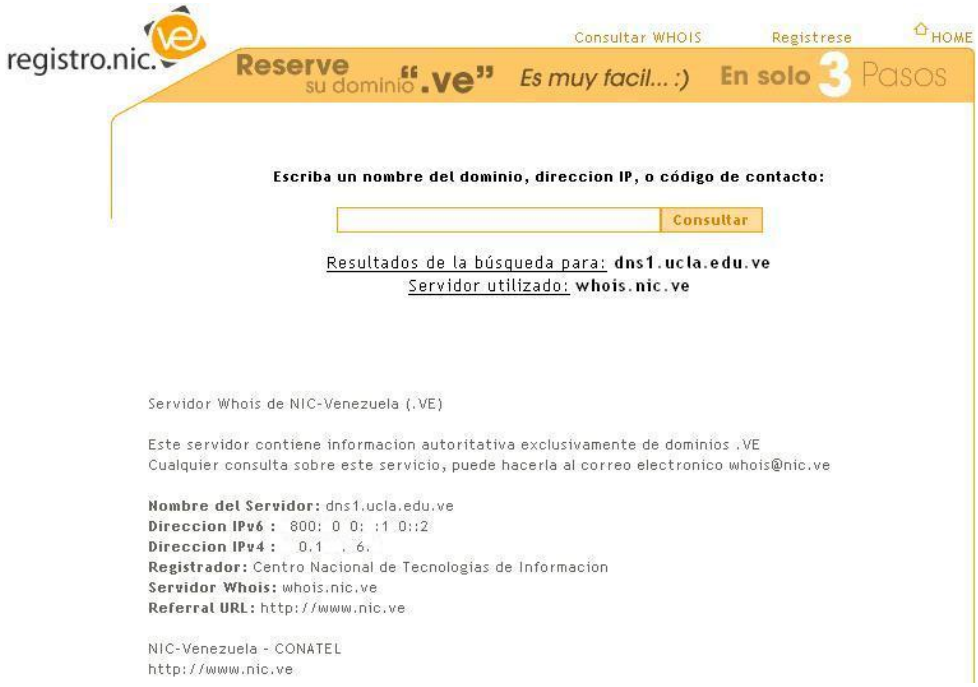

Figura 19: Registro de DNS1 de UCLA con la IPv6**. Fuente:** Autor (2011)**.**

La figura 20 muestra el resultado del registro del DNS2 de la UCLA.

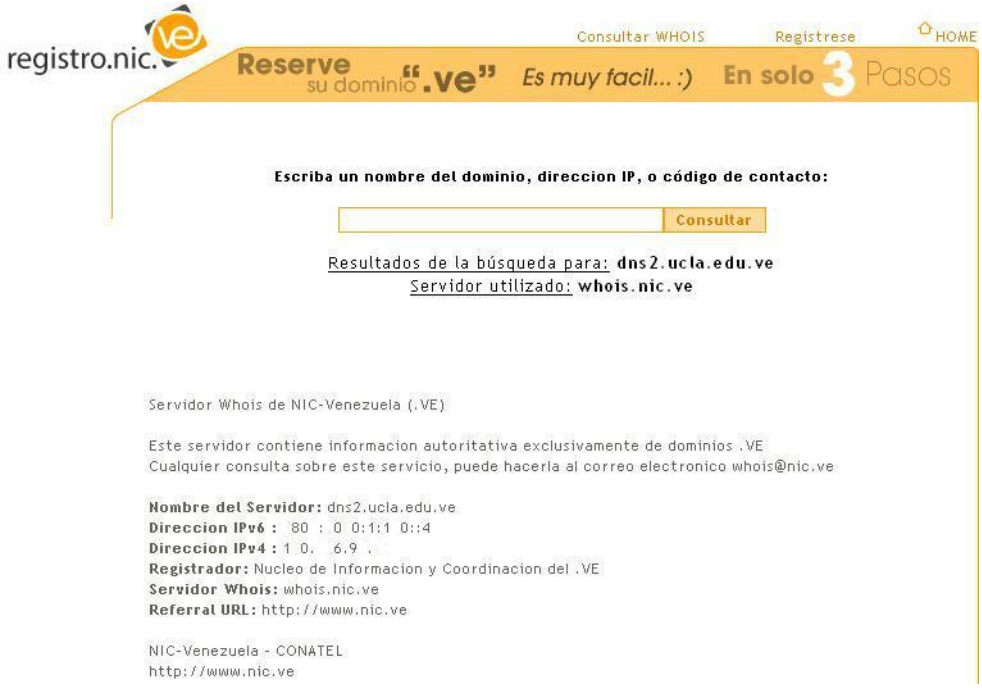

Figura 20: Registro de DNS2 de UCLA con la IPv6**. Fuente:** Autor (2011)**.**

En respuesta al formulario de solicitud a LACNIC, en la que se informó del requerimiento (indicando la información de los DNS's de la UCLA), la delegación del bloque Ipv6 adjudicado a la misma fue realizada por el organismo; permitiendo así que el proceso de resolución inversa fuera posible desde Internet.

Luego de recibidas las respuestas a las solicitudes hechas a cada organismo, se comenzaron a ejecutar pruebas de verificación de los servicios.

Una de las herramientas que se utiliza para examinar el estado de las comunicaciones y enrutamiento se denomina looking glass. El ietfv6 dispone de un sitio web con esta herramienta y desde allí se ejecutaron algunas pruebas que se muestran a continuación.

La figura 21 muestra un traceroute ejecutado desde el ipv6tf con destino al

servidor cofeu.ucla.edu.ve.

```
#traceroute6 -w 3 -m 25   00: 000:1:  1::17

 1  gr2000.consulintel.es (2a01:48:1::ff0)  2.077 ms  2.048 ms  0.665 ms
 2  neosky-consulintel.consulintel.es (2a01:48::d5ac:227d)  29.381 ms  19.248 ms  21.062 ms
 3  2a01:48:100::a (2a01:48:100::a)  23.963 ms  20.203 ms  10.92 ms
 4  xe-0-1-0-6.mad44.ip6.tinet.net (2001:668:0:3::7000:71)  8.056 ms  33.482 ms  7.881 ms
 5  xe-1-1-0.par20.ip6.tinet.net (2001:668:0:2::1:5e2)  28.949 ms  36.496 ms  38.068 ms
 6  xe-4-2-0.was12.ip6.tinet.net (2001:668:0:2::1:13a2)  130.334 ms  122.525 ms  127.249 ms
 7  so-1-0-0.mia11.ip6.tinet.net (2001:668:0:2::11)  138.415 ms  164.289 ms  165.683 ms
 8  brasil-telecom-gw.ip6.tinet.net (2001:668:0:3::8000:b2)  174.659 ms  190.654 ms  187.541 ms
 9  2800:30:ffff:f::2 (2800:30:ffff:f::2)  189.236 ms  188.118 ms  175.364 ms
10  2800:30:ffff:19::3 (2800:30:ffff:1 ::3)  185.336 ms  200.775 ms  207.487 ms
11  2800:a000:ffff:1::1 (  00: 0 0:ffff:1::1)  203.379 ms  205.991 ms  203.364 ms
12  2800:a000:fffd::1 (   0: 0 0:fffd::1)  201.528 ms  207.653 ms  203.945 ms
13  cofeu.ucla.edu.ve (  00: 0 0:1:  1::17)  192.449 ms  197.088 ms *
```

Figura 21 Traceroute a cofeu desde looking glass. **Fuente:** Autor (2011)

La figura 22 muestra un traceroute ejecutado desde el ipv6tf con destino al servidor grado.ucla.edu.ve.

```
#traceroute6 -w 3 -m 25 200:000:1:11::14

 1  gr2000.consulintel.es (2a01:48:1::ff0)  6.614 ms  1.747 ms  0.654 ms
 2  neosky-consulintel.consulintel.es (2a01:48::d5ac:227d)  34.877 ms  7.12 ms  38.406 ms
 3  2a01:48:100::a (2a01:48:100::a)  36.993 ms  6.103 ms  38.789 ms
 4  xe-0-1-0-6.mad44.ip6.tinet.net (2001:668:0:3::7000:71)  77.639 ms  204.853 ms  258.533 ms
 5  xe-1-1-0.par20.ip6.tinet.net (2001:668:0:2::1:5e2)  243.561 ms  117.707 ms  142.333 ms
 6  xe-7-1-0.was10.ip6.tinet.net (2001:668:0:2::1:1142)  253.843 ms  152.666 ms  147.17 ms
 7  xe-4-0-0.mia10.ip6.tinet.net (2001:668:0:2::1:15e2)  158.413 ms  214.017 ms  155.264 ms
 8  brasil-telecom-gw.ip6.tinet.net (2001:668:0:3::8000:b2)  170.135 ms  373.686 ms  405.295 ms
 9  200:30:ffff:f::2 (200:30:fff:f::2)  293.641 ms  185.55 ms  186.448 ms
10  200:30:ffff:19::3 (200:30:fff:19::3)  205.538 ms  202.801 ms  220.871 ms
11  200:000:fff:1::1 (200:a000:ff:1::1)  231.083 ms  260.735 ms  203.524 ms
12  200:000:ffd::1 (200:000:fd::1)  206.388 ms  230.871 ms  257.878 ms
13  postgrado.ucla.edu.ve (800:000:1:11::14)  268.64 ms  198.494 ms *
```

Figura 22 Traceroute a postgrado desde looking glass. **Fuente:** Autor (2011)

La figura 23 muestra un traceroute ejecutado desde el ipv6tf con destino al servidor www.ucla.edu.ve

```
#traceroute6 -w 3 -m 25 200:000:1:11::11

 1  gr2000.consulintel.es (2a01:48:1::ff0)  3.736 ms  1.76 ms  0.647 ms
 2  neosky-consulintel.consulintel.es (2a01:48::d5ac:227d)  24.052 ms  19.655 ms  19.842 ms
 3  2a01:48:100::a (2a01:48:100::a)  26.29 ms  27.409 ms  31.073 ms
 4  xe-0-1-0-6.mad44.ip6.tinet.net (2001:668:0:3::7000:71)  6.878 ms  22.677 ms  31.075 ms
 5  xe-1-1-0.par20.ip6.tinet.net (2001:668:0:2::1:5e2)  46.095 ms  32.097 ms  45.141 ms
 6  xe-8-1-0.was10.ip6.tinet.net (2001:668:0:2::1:1152)  130.29 ms  124.619 ms  126.312 ms
 7  so-1-0-0.mia11.ip6.tinet.net (2001:668:0:2::11)  138.194 ms  159.513 ms  192.327 ms
 8  brasil-telecom-gw.ip6.tinet.net (2001:668:0:3::8000:b2)  321.229 ms  193.567 ms  191.074 ms
 9  2800:30:ffff:f::2 (200:30:ffff:f::2)  187.715 ms  188.243 ms  184.393 ms
10  2800:30:ffff:19::3 (200:30:ffff:19::3)  279.524 ms  231.129 ms  320.609 ms
11  2800:a000:ffff:1::1 (00:000:ffff:1::1)  323.52 ms  225.51 ms  208.34 ms
12  2800:a000:fffd::1 (200:000:fffd::1)  211.767 ms  217.305 ms  203.077 ms
13  www.ucla.edu.ve (200:000:1:11::11)  265.478 ms  200.033 ms *
```

Figura 23 Traceroute a ucla desde looking glass. **Fuente:** Autor (2011)

Se muestra a continuación un traceroute desde un pc en la DMZ2 con destino IPv6 de google.

```
[root@lavecino ~]# traceroute ipv6.google.com
traceroute to ipv6.google.com (2001:4860:8001::6a), 30 hops max, 40 byte packets
 1  * * *
 2  * * *
 3   (200:000:ff:1::2)  3.218 ms  3.222 ms  3.174 ms
 4  200:30:ffff:1::1 (200:30:ff:1::1)  15.086 ms  15.084 ms  15.079 ms
 5  200:30:ffff:f::3 (200:30:ff:f::3)  14.992 ms  14.922 ms  15.083 ms
 6  ae2-132.nyc22.ip6.tnet.net (2001:668:0:3::8000:b1)  54.868 ms * *
 7  * * *
 8  * 2001:4860:1:1:0:cb9:0:c (2001:4860:1:1:0:cb9:0:c)  83.455 ms  83.474 ms
 9  2001:4860::1:0:9ff (2001:4860::1:0:9ff)  84.729 ms 2001:4860::1:0:5dc
(2001:4860::1:0:5dc)  89.142 ms 2001:4860::1:0:9ff (2001:4860::1:0:9ff)  116.226 ms
10  2001:4860::1:0:489 (2001:4860::1:0:489)  99.057 ms * *
11  * * *
12  2001:4860:0:1::d3 (2001:4860:0:1::d3)  99.260 ms * 2001:4860:0:1::d3
(2001:4860:0:1::d3)  101.175 ms
13  gw-in-x6a.1e100.net (2001:4860:8001::6a)  101.261 ms  99.195 ms  101.271 ms
[root@lavecino ~]#
```

La consulta a DNS se ejecutó con el comando Host y sus parámetros correspondientes. Se muestra una consulta al secundario interno :

```
[root@palavecino ~]# host -t aaaa www.ipv6tf.org 200:000:1:12::3
Using domain server:
Name: 200:000:1:12::3
Address: 200:000:1:12::3#53
Aliases:
www.ipv6tf.org has IPv6 address 2a01:48:1:0:2e0:81ff:fe05:4658
```

Para verificar varios parámetros del protocolo IPv6 en sitios web de la Intranet habilitados con el mismo, se utilizó entre otras, la página validador.ipv6.br, publicada por el centro de estudios e investigación en tecnología de redes de Brasil. Este sitio realiza una consulta quad-A para resolver la URL, en caso de que devuelva una dirección IPv6, realiza pruebas DNS. Luego ejecuta un ping6 a la dirección, todo

por medio de un API desarrollada por ese proveedor. Se muestra a continuación un ejemplo de la verificación. La figura 24 muestra el resultado de las pruebas por el sitio validador.ipv6.br hacia el sitio www.ucla.edu.ve.

Figura 24: Validador IPv6 a ucla. **Fuente:** Autor (2011)

La figura 25 muestra el resultado de las pruebas por el sitio validador.ipv6.br hacia los sitios postgrado.ucla.edu.ve y sed.ucla.edu.ve.

Figura 25: Validador IPv6 a seucla y postgrado. **Fuente:** Autor (2011)

El sitio www.vynke.org muestra el despliegue de IPv6 por país y por tipo de organización (Educación, comercio-e, gobierno, ISP, etc.). La figura muestra los prefijos de las Instituciones de Educación en Venezuela y una codificación de colores indicando si se ha efectuado el anuncio en BGP y si se ha observado tráfico desde ese origen. La figura 26 muestra en verde los prefijos anunciados por las Universidades en Venezuela.

- : traffic from this prefix has been seen, **3 (15 %)**
- GREEN: announced on BGP, **9 (45 %)**
- ORANGE: announced on BGP but under an aggregated prefix (such as the ISP rather than the customer), **0 (0 %)**
- RED: not announced on BGP, **11 (55 %)**

Prefix	Description	First/Last announcement
2001:1338::/32	Fundación Centro Nacional de Innovación Tecnológica (CENIT)	2010-09-15
2001:1350::/32	COMSAT VENEZUELA	2011-02-23
2800:30::/32	Fundación Centro Nacional de Innovación Tecnológica (CENIT)	2011-03-02
2800:38::/32	Centro Nacional de Tecnologías de Información (CNTI)	
2800:100::/32	Universidad Simon Bolivar	2011-03-03
2800:140::/32	Private Ip Services	
2800:3e0::/32	Sprint Nextel	2010-12-07
2800:500::/32	Telecomunicaciones MOVILNET	
2800:5e0::/32	Gold Data C.A.	
2800:620::/32	Net Uno, C.A.	
2800:6b0::/32	Telcel, C.A	
2800:6e0::/32	Brasil Telecom de Venezuela, S.A.	
2800:a000::/32	Universidad Centro Occidental Lisandro Alvarado	2011-03-02
2800:a008::/32	Universidad de Los Andes	2011-03-02
2800:a010::/32	Universidad Central de Venezuela	2010-09-15
2800:a018::/32	Universidad de Oriente	
2800:a020::/32	Universidad Pedagógica Experimental Libertador	
2800:a028::/32	Universidad del Zulia	
2800:a030::/32	Universidad de Carabobo	2010-09-15
2800:a038::/32	Universidad Bolivariana de Venezuela	

Figura 26: Prefijos IPv6 en Universidades de Venezuela. **Fuente:** Autor (2011)

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El diagnóstico de la realidad de la Red UCLA en relación a la capacidad en hardware, software, recurso humano capacitado y proveedores de servicio, permitió determinar la factibilidad de la ejecución del presente trabajo de investigación. La investigación documental acerca de los aspectos técnicos involucrados en una etapa inicial de transición al protocolo de Internet de nueva generación nutrió el interés de aplicar tal aprendizaje teórico en actividades tangibles desde el punto de vista práctico. La diversidad de hardware fue un aspecto base en el estudio, tomándose en cuenta la topología de red e interconexiones disponibles. Una vez confirmada la capacidad de hardware en los niveles de la topología de red (Núcleo, Distribución y acceso), se efectuó el análisis de los sistemas operativos y servicios: soporte del protocolo, requerimiento de migración de versiones y parámetros a modificar para la habilitación. Una de las ventajas consistió en la disponibilidad de elementos de comunicaciones administrables, con capacidad de conmutación, la existencia de zonas desmilitarizadas en la configuración de seguridad con posibilidad de agregar funcionalidades del protocolo IPv6. En tal sentido, se hizo evidente que para la escogencia de equipos de red y telecomunicaciones en las etapas iniciales de una red de dato se debe tomar en cuenta el crecimiento futuro en requerimientos de servicios, usuarios siendo una política errada ajustar las características al requerimiento actual sin pensar en el futuro, aunque no sea posible adivinar la cantidad de usuarios que ingresarán al sistema ni la aparición de nuevos protocolos, también es cierto que es posible estimar un aumento de la demanda de servicios. La comunicación con los proveedores de servicio involucrados, su capacidad técnica, de soporte de protocolo y

de respuesta en el corto plazo fueron aspectos importantes durante la implementación, siendo el funcionamiento del servicio de Internet y comunicaciones un engranaje de elementos técnicos que no dependen exclusivamente del departamento especializado en la Universidad y en cualquier empresa.

En función de ejecutar efectivamente la implementación del protocolo IPv6 en un ambiente académico, se requiere realizar una planificación de las tareas necesarias con la finalidad de establecer un orden en el despliegue del protocolo. Un entendimiento de las características de la red en la que se pretende realizar tal trabajo es un requerimiento esencial para desarrollar tal planificación.

Recomendaciones

Siendo IPv6 un protocolo que recién comienza a ver su despliegue a nivel mundial comparado con IPv4 que se encuentra en una etapa de agotamiento; para el caso específico de la UCLA los aspectos que sirven de base para el desarrollo de servicios y aplicaciones en IPv6 fueron ejecutados en la presente investigación.

A pesar de que la tecnología de conmutación a nivel de acceso, distribución y núcleo instalada en la red UCLA funciona para el uso del protocolo IPv6, aspectos como Multicast con protocolo MLD carecen de soporte y se requeriría la migración de dicha plataforma para contar con la disponibilidad de esta característica.

Para futuras adquisiciones de equipos de tecnología de información y comunicaciones sería recomendable que tales elementos posean soporte certificado para el protocolo IPv6, de esta manera se facilitarían las posibilidades de desarrollo aplicaciones y proyectos únicamente posibles con IPv6.

Actualmente existen en el mercado distintos fabricantes que disponen de equipos de administración de direcciones y servicios DNS y DHCP IPv4 e IPv6 (IPAM) con capacidad de redundancia y con hardware exclusivo para tal fin, evitando la dependencia de un sistema operativo y un servidor para instalar una o varias aplicaciones que realicen las funciones descritas. Este tipo de soluciones facilitaría la administración de red, reduciendo el tiempo de respuesta del Departamento de Redes

de Dato y la disponibilidad de especialistas en la distribución de sus funciones.

Para el sistema Operativo Windows, algunas versiones del mismo poseen soporte limitado del protocolo IPv6, quedando demostrado que con la versiones más recientes para cliente (Windows7) y servidor (2008), se facilita el trabajo práctico en la Implementación.

Los sistemas operativos de los firewalls requieren ser evaluados para comprobar el soporte del protocolo IPv6, siendo necesaria su actualización a una versión que cumpla los requerimientos de la red particular.

Un análisis de la plataforma tecnológica en los núcleos foráneos ayudaría a determinar la posibilidad de incluir el desarrollo de proyectos y aplicaciones que aporten soluciones con el protocolo IPv6 y la migración de la plataforma en caso de ser necesario.

REFERENCIAS BIBLIOGRÁFICAS

Obispo, F. (2005). Implementacion de IPv6 en el CNTI.[On-Line]. Disponible en: ipv6tour.lacnic.net/docs/f-obispo-implement-ipv6-cnti.pps. [Consultado Noviembre 2010].

Grossetete P. (2008). Global IPV6 Strategies: From Business Analysis to Operational Planning. CiscoPress, Indianapolis.

Games, *E. (2007).* Implementing IPv6 at Central University of Venezuela. [On-Line].Disponible en: http://portal.acm.org/citation.cfm?id=1384124**.** [Consultado Noviembre 2010].

Jara, F. (2009). Estudio e Implementación de una red IPv6 en la UTFSM. [On-Line] Disponible en: http:// portalipv6.lacnic.net/files/documentos/Implementacion Ipv6_UTFS_proyecto.pdf [Consultado Abril 2011]

Schuh, S. (2006). Migrating Small Business Networks To IPv6 [On-Line]. Disponible en: http://stud3.tuwien.ac.at/~e0000195/DA/DA_gesamt_v1.01.pdf. [Consultado Abril 2011]

Prieto,J. (2008). Implementación de *appliances* para enrutado de IPv6 desde plataformas *hardware* económicas. [On-Line]. Disponible en: http://eprints.ucm.es/9216/1/Memoria_Complu6ix_III.pdf. [Consultado Abril 2011]

Davies, J. (2008). Understanding IPv6. Microsoft Press, Washington.

Amoss, J. (2008). Handbook of IPv4 to IPv6 Transition. Aurebach Publications. Boca Raton, FL.

ANEXOS

ANEXO "A". Formato de observación estructurada

Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Conectividad física	Estado de conectividad en equipos de comunicaciones	Interfaces ATM en Router de conexión al proveedor	Conectadas
		Interfaces para IBGP	Conectadas
		Interfaces de conectividad Troncal en conmutadores core de la red	Con conexión
		Interfaces de distribución y acceso en conmutadores	Con conexión
Equipos Servidores y estaciones para pruebas	Observar la capacidad de hardware de los equipos para pruebas.	Capacidad de memoria en Equipos virtuales (servidores y estaciones) donde se realizaron pruebas iniciales de funcionamiento de servicios	AL menos 1Gb
		Capacidad de almacenamiento en Equipos virtuales (servidores y estaciones) donde se realizaron pruebas iniciales de funcionamiento de servicios	Al menos 10Gb

Continuación Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Equipos Servidores y estaciones para pruebas	Observar la capacidad de hardware de los equipos para pruebas.	Cantidad de procesadores (CPU)	Máximo dos
		Velocidad del reloj del (los) CPU (GHz)	Al menos de 1,3GHz
Equipos en producción	Observar la capacidad de hardware de los servidores	Capacidad de memoria Ram	Al menos 4 Gb
		Capacidad de almacenamiento	Al menos 20 Gb
		Cantidad de procesadores (CPU)	Al menos dos
		Velocidad del reloj del (los) CPU (GHz)	Al menos 1,3 GHz
Funcionali-dad del Sistema Operativo	Observar la disponibilidad de soporte IPv6 en los sistemas operativos de los equipos que intervienen en la Implementación	Sistema operativo de firewalls	Versión 3MR5: IPv6 No Soportado
		Sistema Operativo de Routers de borde	IPv6 Soportado

Continuación Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Funcionali-dad del Sistema Operativo	Observar la disponibilidad de soporte IPv6 en los sistemas operativos de los equipos que intervienen en la Implementación	Sistema Operativo de conmutadores Core, Distribución y Acceso	IPv6 a nivel de capa 3 no requerido para esta topología, transparente a nivel de capa 2
		Sistema Operativo Linux Centos	Kernel 2.6.18 IPv6 soportado
		Sistema Operativo Windows XP	Sin Cliente DHCPv6
		Sistema Operativo Windows 7	Soportado
		Sistema Operativo Windows 2003	Soportado
		Sistema Operativo Windows 2008	Soportado

Continuación: Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Funcionali-dad del Sistema Operativo	Observar el estado de configuración del protocolo IPv6 en los equipos que intervienen en la implementación	Sistema Operativo de Routers de borde	No configurado
		Sistema Operativo de Firewalls	No configurado
		Sistema Operativo de conmutadores	No configurado
		Sistema Operativo de servidores	No configurado
		Sistema Operativo de estaciones	No configurado
Requerimien-to de Actualización de Sistema Operativo	Determinar la necesidad de efectuar actualizaciones de sistemas operativos en los elementos que forman parte de la Implementación	Sistema operativo de firewalls	Actualización a versión 4MR2
		Sistema Operativo de Routers de borde	No requerido
		Sistema Operativo de conmutadores Core, Distribución y Acceso	No requerido
		Sistema Operativo Linux Centos	No requerido
		Sistema Operativo Windows XP	Actualización a Windows 7

Continuación: Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Requerimiento de Actualización de Sistema Operativo	Determinar la necesidad de efectuar actualizaciones de sistemas operativos en los elementos que forman parte de la Implementación	Sistema Operativo Windows 7	No requerido
		Sistema Operativo Windows 2003	No requerido
		Sistema Operativo Windows 2008	No requerido
Funcionali-dad de servicios	Observar el soporte del protocolo IPv6 a nivel del servicio DNS en los equipos que intervienen en la implementación	Servicio BIND	Soportado

Continuación: Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Funcionali-dad de servicios	Observar el soporte del protocolo IPv6 a nivel del servicios DHCPv6 en los equipos que intervienen en la implementación	Servicio DHCPv6	No soportado para software CNR ni Windows 2003 Server. Soportado para IOS cisco y Windows Server 2008
	Observar el soporte del protocolo IPv6 a nivel del servicios Web en los equipos que intervienen en la implementación	Servicios Web IIS 7 y Apache 2.2	Soportado para ambos casos

Continuación: Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Requerimien-to de Actualiza-ción de Servicios	Determinar la necesidad de efectuar actualizaciones de los servicios que forman parte de la Implementación	Servicio BIND Servicio DHCPv6 Servicios Web IIS 6 y Apache 2.2	No requerida Instalación de servicio DHCPv6 en sistema Windows Server 2008 No requerida
Normas de comunicación	Observar la existencia de un número de sistema autónomo para la UCLA	Configuraciones en routers de borde	Sistema autónomo presente
Software	Soporte de protocolo de enrutamiento dinámico	BGP hacia el proveedor	Soportado

Continuación: Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Hardware	Estado de conectividad de última milla	Equipos, interfaces y elementos de conectividad del proveedor en sala de comunicaciones de la UCLA	Presentes
Soporte técnico	Capacidad de respuesta del proveedor para configuraciones conjuntas con UCLA	Notificaciones de respuesta del soporte técnico del proveedor	Respuesta positiva en un intervalo corto de tiempo

Continuación: Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Componentes, módulos, tarjetas	Observar las tarjetas, componentes y módulos presentes en router con conectividad al proveedor de Internet Comercial	Módulos (con soporte IPv6 documentado por el fabricante) instalados en los slots del Router	Instalada Supervisor Engine 720 Rev. 5.4 Instalada Port adapter Enhanced FlexWAN Rev. 2.3.
	Observar las tarjetas, componentes y módulos presentes en router con conectividad al Proveedor de la red Académica Reacciun2	Módulos (con soporte IPv6 documentado por el fabricante) instalados en los slots del Router	Network Processing Engine NPE-G1 ATM WAN OC3 SMI Port Adaptor

Continuación: Formato de Observación: Variable Dependiente

Indicadores	Item	Elementos de Observación	Resultado
Modelo del equipo	Número de parte del equipo	Número de parte observable en la configuración de los equipos	3600, 200A .Procesadores compatibles IPv6 y soportan implementaciones Dual Stack y Tunnel
Modelo del equipo	Número de parte del equipo	Número de parte observable en la configuración de los equipos	WS-C3750G-24TS, WS-C2960-24TT-L, WSC4006

Fuente: Autor (2011)