Universidad Latinoamericana de Ciencia y Tecnología
Facultad de Ciencia y Tecnología
Escuela de Ingeniería
Licenciatura en Ingeniería Informática

Hacia la siguiente generación del Protocolo de Internet

Randall Hernández Solano
1-0879-0824

Proyecto de Graduación para optar por el grado de Licenciatura en Informática
con énfasis en Redes y Sistemas Telemáticos

San José, Costa Rica
Octubre, 2004

Introducción

Desde sus inicios, el Internet ha evolucionado muy rápido hasta llegar a la popularidad con que cuenta hoy en día. Lo que comenzó como una red, sobre todo con fines experimentales, científico-técnicos y, por supuesto, con objetivos militares en los Estados Unidos, ha terminado convirtiéndose en uno de los más populares sistemas de comunicación en el ámbito mundial del momento. Esto ha creado una serie de nuevos desafíos que la comunidad tecnológica ha tenido que afrontar.

El espectacular crecimiento del tráfico en Internet y la tan ansiada convergencia de voz, datos, imagen y la integración de una impensable cantidad de servicios en una única red, hacen necesaria una evolución de las comunicaciones que, según los analistas, irá de la mano de las siglas IP. Sin embargo, la necesidad de contar con una única red a través de la cual pueda viajar toda esa información; en la que converjan todas nuestras comunicaciones (voz, datos y contenidos multimedia), aparece actualmente como un elemento crítico que marcará el funcionamiento de la Sociedad de la Información.

El Protocolo de Internet "IP", el lenguaje en el que "habla" la Red, aparece como el pilar o el elemento integrador, capaz de hacer converger todas las necesidades de comunicación de compañías y usuarios en una misma infraestructura. La necesidad de interconexión y de una gestión centralizada de la información de una empresa es otra de las exigencias de la Nueva Economía que nos lleva necesariamente a la adopción de IP como elemento integrador.

Existe, como se ve, una gran coincidencia en señalar a IP como el elemento que permitiría llegar a esta realidad. Pero ante esta posibilidad surgen grandes preguntas: ¿Cuáles son las razones que le hacen merecedor de tanta confianza? ; ¿cuál es la diferencia en entre el IP de hoy y el que necesitamos?, ¿cuáles son las ventajas y desventajas?, ¿cuáles medidas se han tomado en nuestro país al respecto?, ¿cuánto sabe la comunidad informática costarricense al respecto? , ¿estamos preparados?.

Estas y otras interrogantes son la motivación del presente estudio el cual se propone convertirse en una guía para enfrentar el cambio "Hacia la siguiente generación del Protocolo de Internet".

Agradecimiento

En primer lugar agradezco a Dios por permitirme concluir una más de mis metas, dándome fuerza y voluntad para luchar contra las dificultades que en una u otra forma se me presentaron.

A mis compañeros de trabajo, profesores y amigos, que con sus comentarios, opiniones y consejos dieron su ayuda y apoyo incondicional a este proyecto.

Al Lic. Rodney Herrera, mi tutor por todas las cosas que me ha enseñado y por su gran colaboración y ayuda.

¡Que el señor les bendiga; un millón de Gracias!

Dedicatoria

Ante todo a Dios por ayudarme día a día en todos los aspectos de mi vida, por haberme dado la familia que me dio y en este momento por permitirme lograr una más de mis metas.

A mi madre, mis hermanos y amigos que me han apoyado siempre en todo momento y por el cariño que siempre me han demostrado.

TABLA DE CONTENIDO

1. Aspectos situacionales

1.1 Antecedentes

La red Internet, basada en un diseño de principios de los años 80, ha experimentado un crecimiento sin precedentes en la historia de las telecomunicaciones, tanto en número de usuarios conectados como en aplicaciones y servicios disponibles.

Así mismo, es bien sabido que han aparecido deficiencias en los aspectos administrativos y de seguridad, así como carencias en lo referente a la futura prestación de servicios avanzados.

A la hora de diseñar un método de asignación de direcciones en los albores de Internet, cuando estaba conectada apenas una docena de centros, se pensó en un esquema basado en el tamaño de las organizaciones (de esa época) y de ahí nació el modelo de clases en la que sólo se daba cabida a tres tipos de prefijos de longitud predeterminada según fuera una gran organización (clase A, prefijo 8 bits), de tamaño mediano (clase B, prefijo 16 bits) o pequeño (clase C, prefijo 24 bits). Existen entonces 128 prefijos correspondientes a clases A (0.0.0.0/8-127.0.0.0/8), 16384 de clases B (128.0.0.0/16-191.255.0.0/16) y algo más de 2 millones de clases C (192.0.0.0/24-223.255.255.0/24).

La asignación de direcciones comenzó a hacerse de manera centralizada por un único centro de registro (SRI-NIC) satisfaciendo casi todas las solicitudes sin necesidad de mayor trámite. Este modelo de asignación de direcciones, cuando Internet comenzó a crecer de forma espectacular, trajo algunas de las siguientes consecuencias:

- Mal aprovechamiento del espacio de direcciones. Cada centro tendía a pedir una clase superior a la requerida, normalmente una clase B en vez de una o varias clases C, por puro optimismo en el crecimiento propio o por simple vanidad.

- Peligro de agotamiento de las direcciones de clase B; las más solicitadas, debido a la escasez de posibilidades de elección. La alerta sonó cuando se había agotado el 30% de esta clase y la demanda crecía exponencialmente.
- Síntomas de saturación en los routers de los backbones. Al imponerse restricciones severas en la asignación de clases B, las peticiones de múltiples clases C se hicieron masivas, lo que hizo que aumentara de forma explosiva el número de prefijos que los routers habían de mantener en sus tablas, y se llegaron a alcanzar los límites físicos impuestos por la capacidad de memoria y de proceso.

Por tanto, se da ante un doble problema: agotamiento de direcciones y colapso de routers debido a la explosión de rutas. En una situación en la que la población conectada a la red se duplicaba (en términos de equipos y redes conectadas) en periodos que oscilaban en torno a los 6 meses, había que tomar medidas urgentes, y he aquí algunas:

- Imposición de políticas restrictivas de asignación de direcciones por parte de los centros de registros (ya descentralizados del primitivo NIC).
- Modificación de los protocolos exteriores de enrutamiento para soportar prefijos de red variables.
- Para entender bien el problema hay que tener en cuenta que el periodo en el que los fabricantes duplican la capacidad de proceso de sus equipos y la de sus memorias es de aproximadamente dos años. La capacidad de los routers que deben mantener en sus tablas una información completa o full-routing sobre la topología de Internet "equipos conectados a los backbones principales o de dominios conectados a múltiples proveedores" se habría hoy superado, con el colapso consiguiente de Internet, si el método de asignación de prefijos variables no hubiese sido puesto en funcionamiento a principios de 1994. En este momento existen más de 60.000 redes conectadas, mientras que los equipos que soportan full-routing manejan alrededor de 30.000 prefijos.

De forma repetida se ve cómo se achaca a Internet el ser un medio de comunicación inseguro. Este es un tema con muchos ángulos y que debe ser examinado en cada una de sus partes. Dado el carácter puramente académico de Internet en su comienzo, los asuntos relativos a la seguridad fueron, como desgraciadamente suele ocurrir en la práctica, relegados a posterior estudio hasta que los primeros ataques globales hacen sonar la alarma y empieza a producirse un notable esfuerzo en incorporar mecanismos de seguridad a las aplicaciones existentes, el problema de seguridad en el nivel de red sigue sin ser tomado en cuenta y comienza a producirse una serie de ataques cada vez más sofisticados y basados en la suplantación de la identidad de máquinas conectadas a la red, dando la posibilidad de violar un acceso prohibido o la posibilidad de escudriñar (o desviar) la información a intrusos. Como respuesta surgieron mecanismos de barrera como los cortafuegos , pero los protocolos siguen sin incorporar medidas específicas de seguridad.

Pero esto es sólo una parte del problema. La seguridad integral comprende servicios tanto de confidencialidad como de autentificación, integridad y no rechazo para los que se requieren técnicas de encriptación que están sujetas a diferentes normativas de exportación y utilización en determinados países, lo que hace complicado su uso generalizado en un medio que se tiene por libre y homogéneo (en cuanto al tipo de protocolos y aplicaciones empleados). Se corre el peligro de fracturar Internet en zonas donde se pueda intercambiar información de forma segura y otras en que no, bien por considerarse tecnología de uso militar, bien por el derecho que se guardan algunos gobiernos a poder intervenir -e interpretar- las comunicaciones de sus ciudadanos.

En otro orden de cosas, estamos asistiendo al nacimiento de servicios de transmisión de información en tiempo real dentro de Internet. Ejemplos de ello son las aplicaciones para comunicaciones de voz a través de la red, red virtual superpuesta a Internet, basada en el concepto de IP Multicast . Un defecto claro de IPv4 es la falta de caracterización de los distintos flujos de información que viajan por la red, sujeto a la redundancia de un mecanismo corrector de transporte, que en una transmisión de voz en tiempo real en la que la pérdida de un número significativo de paquetes puede alterar o incluso imposibilitar la interpretación de la información. La aparición de este

tipo de servicios en la era de las autopistas de la información presenta una clara limitación al uso de el Internet tal y como se concibe actualmente.

En cualquier caso, hay que entender que tanto la asignación de prefijos de longitud variable, como las políticas restrictivas de asignación de direcciones son sólo medidas temporales, dirigidas a afrontar problemas concretos y que no resuelven (en algunos casos hasta agravan) los problemas crónicos detectados en Internet en gran parte debido a su tremendo éxito. Así, se han llegado a plantear iniciativas como la devolución de direcciones, la obligatoriedad de cambiar de direcciones al cambiar de proveedor, la asignación dinámica de direcciones, el uso de traductores de direcciones (NAT) que transformen un espacio privado de direcciones en otro perteneciente al proveedor, o incluso el cobrar una cantidad elevada por cada prefijo (no perteneciente al espacio del proveedor) que un cliente desee que su proveedor anuncie

Para remediar estos males, los cuerpos técnicos de Internet impulsaron un debate bajo el lema de IP Next Generation (IPng) que ha culminado con la especificación de un nuevo protocolo IP, sucesor del actual IPv4, y conocido formalmente como la versión 6 del Protocolo Internet o IPv6.

1.2 Justificación

La red Internet, basada en un diseño de principios de los años 80, ha experimentado un crecimiento sin precedentes en la historia de las telecomunicaciones tanto en número de usuarios conectados como en aplicaciones y servicios disponibles.
Internet ha crecido exponencialmente desde 1990, a medida que cada vez más organizaciones entran en el ciberespacio en busca de negocios, facilitando la investigación y ofreciendo formación. La otra cara de este fenomenal éxito es que Internet se enfrenta a una seria escasez de direcciones IP, esas cadenas únicas de números binarios que identifican a las máquinas en Internet. A principios de los 90 se predijo que las últimas Clases B de direcciones IP serían asignadas en marzo de 1994, un mes apodado "Fecha del Juicio Final ". Aunque los investigadores desarrollaron soluciones provisionales para posponer el "Día del Juicio Final", hoy está ocurriendo

otra vez lo mismo: todas las direcciones IP actuales se agotarán en algún momento entre el 2005 y el 2010, si la tasa de crecimiento de Internet continúa.

En lo personal considero impresionante que ante un cambio tan importante que afectará a todas las empresas de cualquier tipo, tamaño u actividad se permanezca sin tomar en cuenta su verdadera trascendencia ya que las empresas deben tenerlo como base para sus planes de expansión y modernización y por qué no para su permanencia en el mercado como un ente competitivo. Hace poco tiempo hubo un acontecimiento similar con igual importancia; este fue el anunciado cambio del año 2000 "Y2K" el cual fue superado con un alto grado de certeza gracias a que se promulgó con suficiente tiempo y las diferentes empresas y usuarios de todo tipo pudieron tomar las previsiones y hacer los ajustes y o correcciones necesarias a sus sistemas. En este caso tal vez la indiferencia se deba a que no se ha puesto una fecha límite para realizar el cambio como en el anterior. En Costa Rica poco o casi nada se ha escuchado hablar del tema; por eso mi empeño mediante este trabajo de informar a la sociedad costarricense y motivar a la comunidad informática para que lo tome en cuenta ya que no debemos permitir que la modernización y los cambios tecnológicos nos pasen por encima. Más bien debemos utilizarlos como una fuerte herramienta para el crecimiento y expansión de las empresas; aprovechando de la mejor manera el aumento en la calidad de los servicios, como las comunicaciones de voz a través de la red y las mejoras en seguridad que fortalecen áreas como el comercio electrónico y nos permiten el mejor manejo descentralizado de información vital para la empresa; así como también un incremento considerable en las velocidades de transmisión. En general, todos los servicios que hoy son parte imprescindible de nuestras vidas en un mundo globalizado se verán beneficiadas con las mejoras introducidas en "el nuevo protocolo de Internet ".

Por todo lo anterior, es necesario que la comunidad informática cuente con un compendio de información acerca del tema que facilite su comprensión e impacto a nivel mundial y a la vez le ayude a dar ese paso cada vez más inminente y así poder explotarlo de una manera positiva.

Finalmente, el nuevo protocolo de Internet IPv6 o IPng, un protocolo obtenido del estudio de las limitantes de la versión actual de IP y que promete incluir un número

inimaginado de personas y servicios dentro de los servicios de Internet, será la forma de comunicación más importante del siglo XXI.

1.3 Estado de la Cuestión

Breve Historia de IPv6

Varios grupos de trabajo han elaborado propuestas con el fin de diseñar el nuevo IP: la primera fue reemplazar IP por el protocolo CLNP ("ConnectionLess Network Protocol" Protocolo de Red sin conexión) del servicio de red de OSI ("Open System Interconnection" Intercone xión de Sistema Abierto). Esta propuesta denominada TUBA ("TCP y UDP over Bigger Addresses" TCP y UDP bajo direccionamiento amplio) hubiera permitido la convergencia de OSI e Internet.

Sin embargo, numerosos miembros del IETF "Fuerza de la ingeniería de Internet" rebatieron los intentos de imponer CLNP. Reaccionaron con otras propuestas tales como IP sobre IP, SIP (Simple IP "IP simple") y PIP ("P" Internet Protocol" El protocolo P de Internet).

Después, IP sobre IP evolucionó rápidamente para dar vida a una nueva propuesta, IPAE ("IP Address Encapsulation" Encapsulamiento de direcciones IP). IPAE fue después adoptado como una estrategia de transición del IP actual hacia SIP. SIP proponía principalmente aumentar el tamaño de las direcciones IP.

En cuanto a PIP, éste proponía una estrategia de encaminamiento más innovadora que permitiese una implementación eficaz del encaminamiento prioritario y que facilitase la movilidad. Los partidarios de SIP y de PIP fusionaron sus propuestas en septiembre de 1993.

El resultado, SIPP (Simple IP Plus), intentaba preservar tanto la eficacia de las codificaciones de SIP como la potencia de los encaminamientos de PIP. Paralelamente, durante todo este tiempo se desarrolla una tercera propuesta, CATNIP ("Common

Architecture for the Internet" Arquitectura común para el Internet) que integraba CNLP, IP e IPX ("Internet Packet exchange" Intercambio del paquete del Internet).

IETF optó finalmente por SIPP, que servirá de base a Ipng "La próxima generación del protocolo de Internet ". Sin embargo, las cualidades y los defectos propios de las otras especificaciones han sido tenidos en cuenta para mejorar la definición del futuro protocolo.

Así, SIPP debe tener algunas modificaciones: su campo "dirección" tiene que pasar de 8 a 16 bytes, la autoconfiguración de las direcciones y deben ser revisados el soporte de la función de movilidad y de Source Routing.

SIPP conserva las direcciones de tamaño fijo (pero más grande) de IPv4 (versión 4 del protocolo de Internet), suprime varios campos con semántica mal definida o que nunca fueron realmente utilizados y añade otros nuevos. Los campos no concernientes a los routers (información de fragmentación, autenticación, entre otros) están colocados después de la cabecera principal en las cabeceras de extensión.

Ipv6 en Costa Rica

En Costa Rica muy poco o casi nada se ha hecho con respecto al nuevo protocolo de Internet. En el momento de la realización de este trabajo solamente se han encontrado pequeñas investigaciones de tipo privadas y casi con carácter personal sobre el tema y a la fecha no se ha logrado constatar la utilización del nuevo protocolo ni siquiera a manera de prueba o en laboratorios institucionales.

IPv6 en Estados Unidos

Estados Unidos no tiene prisa en actualizar el protocolo existente de Internet. IPv4 a IPv6 (Internet Protocol Version 6). Del total global de 4.300 millones de direcciones IPv4 aún quedan mil millones disponibles. Sin embargo, algunas regiones del mundo, y países específicos como Corea del Sur, India y China, comenzarán a experimentar problemas específicos motivados por la carencia de direcciones IP en un plazo estimado en dos años más. La causa de ello radica en que a tales países se ha asignado un

número relativamente bajo de direcciones IP en relación con su densidad demográfica y expectativas de crecimiento en el uso de Internet.

Según la publicación News.com, han de pasar varios años antes que Estados Unidos sienta la necesidad de promover la adopción de IPv6. Eso se debe a que concentra el 70% de los 4.300 millones de direcciones IPv4.

IPv6 en México

En México se inician investigaciones en la materia desde diciembre de 1998, fecha en la que se constituye el proyecto IPv6 en la Universidad Autónoma de México (UNAM), y durante el segundo semestre de 1999 es notable el liderazgo de la UNAM en el ámbito nacional. Dentro del Proyecto IPv6 de la UNAM se estableció un amplio programa de pruebas y trabajos con temas como: implementaciones, stacks IPv4/IPv6, túneles, software de conexión, aplicaciones multimedia, servidores para Web y DNS, autoconfiguración, calidad de servicio, IPv6 sobre ATM, conexión con redes internacionales de IPv6 (6Bone, 6REN), IPv6 en Internet2.

Dentro de las primeras pruebas realizadas destaca la de conexión a 6Bone, la cual es una red mundial experimental utilizada para probar los conceptos y la puesta en operación de IPv6. Actualmente participan en 6Bone en el ámbito mundial 47 países, entre ellos México, donde la UNAM fue el primer nodo en el país, se registra en junio de 1999.

Posteriormente en septiembre de 1999 la UNAM fue aceptada como uno de los 68 nodos de Backbone que a la fecha operan en 6Bone, y obtuvo un rango de direcciones tipo pTLA: 3ffe:8070::/28. Cabe destacar que con este hecho la UNAM es el primer nodo, y hasta el momento el único de este tipo en México, y el tercero en Latinoamérica. Adicionalmente, la UNAM puede delegar direcciones y configurar túneles a instituciones en México y en el mundo interesadas en realizar pruebas con IPv6.

Para contar con una red de pruebas en una primera etapa, y posteriormente con una red de producción, se instaló la Red IPv6 de la UNAM, la primera red IPv6 instalada en México que inició operaciones en agosto de 1999. Cuenta con varios túneles hacia otros nodos de Backbone de 6Bone: SPRINT, FIBERTEL, MERIT, BAY NETWORKS, JANET e ISI-LAP, y hacia los hosts que tiene la UNAM corriendo con sistemas operativos como Win NT4, Win 2000, Solaris y Linux.

Actualmente se esta trabajando con instituciones mexicanas y de América Latina para realizar su conexión IPv6 hacia la UNAM. Entre estas se destacan: Instituto Politécnico Nacional, Universidad Autónoma Metropolitana, Instituto Tecnológico de Estudios Superiores de Monterrey, Universidad Autónoma de Chiapas, Universidad Autónoma de Guerrero, Universidad Autónoma del Estado de Hidalgo, Universidad Autónoma de Nuevo León, Instituto Tecnológico de Oaxaca, Instituto Tecnológico de Mérida, Instituto Tecnológico Autónomo de México, y otros.

Entre las instituciones latinoamericanas están: Instituto de Informática de la Universidad Austral de Chile.

IPv6 en Japón

Japón emitió la directriz política en el otoño del 2000 en un discurso político emitido por el Sr. Yoshiro Mori, Primer Ministro. El gobierno japonés asignó la incorporación de IPv6 y puso una fecha tope del 2005 para la actualización de los sistemas existentes en cada negocio y sector público. Japón ve IPv6 como una de las maneras de ayudarse mediante la influencia de el Internet para rejuvenecer la economía japonesa.

Cisco Systems e IPv6

Como líder reconocido en IP Packet Forwarding, Cisco ha ayudado a progresar con rapidez IPv6 por más de una década a través de innovación constante, esfuerzos de estándares y desarrollo de producto. Cisco ha desarrollado software, hardware,

servicios y entrenamiento de extremo-a-extremo soportando IPv6 para redes futuras. El software Cisco IOS ofrece la base para la integración y co-existencia de IPv6 en Internet. Esto significa que las redes basadas en Cisco son conscientes de IPv6 y permiten la coexistencia entre IPv4 e IPv6, de manera que los clientes pueden configurar IPv6 cuando se requiera. Para información detallada sobre los esfuerzos de Cisco alrededor de IPv6, ir a http://www.cisco.com/ipv6

En los últimos meses, Cisco ha estado activo en el lanzamiento de implementaciones IPv6 a gran escala, tales como SURFnet5. SURFnet5 es la red avanzada de banda ancha de nueva generación de SURFnet, la organización de la red nacional de investigación de Holanda, y es la primera red en Europa que ofrece servicio de Internet en IPv6 nativo. Para ofrecer redes de carga dual, SURFnet5 combina el software Cisco IOS IPv6 con los routers para Internet Cisco 12416. Con el IPv4 y el IPv6 funcionando en una implementación de doble carga, un usuario SURFnet5 puede utilizar uno o ambos protocolos de manera simultánea.

6NET es el proyecto de investigación de Internet más importante en Europa y su objetivo es implementar y probar IPv6 en condiciones reales. Representa una variada combinación de organizaciones industriales y de investigación; existen 31 socios del proyecto que forman parte de 6NET.

Como el principal proveedor de equipo de redes de este proyecto, Cisco ofrecerá una amplia infraestructura de redes IPv6 a través de routers y switches que utilizan el software Cisco IOS en la red IPv6 en funcionamiento más grande del mundo hasta la fecha.

El proyecto 6NET abarcará inicialmente, ocho naciones de Europa y establecerá enlaces con otras iniciativas IPv6 en las regiones de Norteamérica y Asia. 6NET ofrecerá servicios y capacidades IPv6 a, por lo menos, 11 redes nacionales educativas y de investigación. Más adelante se espera que esto se aplique a América Latina.

1.4 Alcances y Limitaciones

1.4.1 Alcances

- Se tratará de difundir el presente estudio a la comunidad informática costarricense por medio del Colegio Profesional y el Ministerio de Ciencia y Tecnología.
- El presente estudio es de carácter informativo acerca del tema (características, estado y compatibilidad); él no pretende ser un manual explicativo de cómo hacer el cambio de versiones del protocolo de Internet.

1.4.2 Limitaciones

- No se tratará en este trabajo sobre aspectos técnicos acerca de la arquitectura de las redes de las empresas de Costa Rica debido a su diversidad (tamaño, actividades y servicios).

1.5 Problema

¿ Cómo debe la comunidad informática costarricense prepararse para el cambio hacia la siguiente generación del protocolo de Internet?

1.6 Objetivos

1.6.1 Objetivo General de diagnóstico

Recopilar y brindar información sobre la nueva generación del protocolo de Internet (Ipv6).

1.6.2 Objetivos Específicos de diagnóstico

1. Conocer el hardware y sus tendencias actuales en cuanto a direccionamiento de datos.

Variables

- Hardware actual y sus tendencias

Definición conceptual

Hardware : Componentes, conjuntos o partes físicos que integran la parte tangible de una computadora o equipo.

Tendencias : Propensión o inclinación en los hombres y en las cosas hacia determinados fines.

Definición oper ativa

Hardware : se refiere a los equipos computacionales (computadoras personales, portátiles y dispositivos como impresoras de red) los cuales intervienen indirectamente (como objetos enrutados) en el proceso de direccionamiento.

Tendencias : se refiere a la inclinación o tendencia hacia ruta en cuanto a progreso y modernización de los equipos.

Instrumento de medición

- Revisión de documentación existente en el mercado.

2. Conocer el software y sus tendencias actuales en cuanto a direccionamiento de datos.

- Software actual y sus tendencias

Definición conceptual

Software: componentes, conjuntos o partes lógicas que integran la parte intangible de una computadora o equipo.

Tendencias : propensión o inclinación en los hombres y en las cosas hacia determinados fines.

Definición operativa

Software: se refiere la parte lógica presente en los equipos computacionales (sistemas operativos y aplicaciones comerciales).

Tendencias : se refiere a la inclinación o tendencia hacia ruta en cuanto a progreso y modernización del software.

Instrumento de medición

Revisión de documentación existente en el mercado.

3. Conocer el software y hardware de comunicaciones y sus tendencias actuales.

   - Software de comunicaciones
   - Hardware de comunicaciones

Definición conceptu al

Software de comunicaciones: componentes, conjuntos o partes lógicas que integran la parte intangible de una computadora y que se utilizan para comunicarse con otros dispositivos y así formar una red de cómputo.

Hardware de comunicaciones: componentes, conjuntos o partes físicas que integran la parte tangible de una computadora o equipo y permiten la comunicación entre dispositivos formando una red de cómputo.

Definición operativa

Software de comunicaciones: se refiere la parte lógica (programas, procesos, protocolos) presentes en los equipos de comunicación, los cuales intervienen en forma activa en el proceso de direccionamiento y de integración de una red como tal.

Hardware de comunicaciones: se refiere a los equipos de comunicaciones (switches, routers y dispositivos) que intervienen en forma activa en el proceso de direccionamiento e integración de la red de comunicaciones.

Instrumento de medición

Revisión de documentación existente en el mercado.

4. Determinar las necesidades en cuanto a recursos humanos requeridos para el cambio.

Variables

- Recurso Humano

Definición conceptual

Recurso Humano: conjunto de las personas que trabajan en un mismo organismo, dependencia o empresa.

Definición operativa: personas o personal de la empresa ya sean técnicos, ingenieros o administrativos y el papel que juegan en el proceso de cambio.

Instrumento de medición

- Revisión de documentación e investigación de requerimientos con respecto al tema.

5. Definir qué aspectos deben considerarse para precisar el Costo\Beneficio del cambio de IP v4 a IP v6.

Variables

- Costo/Beneficio

Definición conceptual

Costo/Beneficio: se refiere a la relación proporcional entre el gasto o costo que se paga a cambio de recibir un bien o servicio y la retribución o ganancia que se obtiene por este.

Definición operativa

Costo/Beneficio : se refiere a la relación directa en cuanto a gasto o inversión que se hace para el cambio y la retribución o ganancias o ventajas que va a dejar percibir a la o las empresas ya sean económicas, personales o de cualquier tipo; como por ejemplo valores agregados.

Instrumento de medición

- Revisión de documentación acerca de costos y beneficios de la implementación.

6. Determinar las implicaciones administrativas que genera el cambio de IP v4 a IP v6.

Variables

- Implicaciones administrativas

Definición conceptual

Implicaciones : Acción o efecto derivado de un proceso.

Definición operativa

Implicaciones : efectos y acciones por tomar por el área administrativa (gerencia, presidencia, directiva) para la ejecución del cambio de versiones del protocolo de Internet en la o las empresas.

Instrumento de medición

- Revisión de documentación sobre implicaciones del cambio.

Objetivo General de Solución

Preparar a la comunidad informática costarricense acerca del próximo cambio en el direccionamiento IP de la versión 4 hacia la versión 6.

Objetivos Específicos de solución

Crear una documentación actualizada que informe con respecto al cambio de la versión 4 del protocolo de Internet a la versión 6.

Variables

- Documentación Actualizada

Definición conceptual

Documentación Actualizada: conjunto de documentos o recopilaciones que acreditan algo o se refieren a un tema en particular y que estén de acuerdo con su fecha de creación.

Definición operativa

Documentación Actualizada: documento creado mediante el estudio y recopilación de información acerca del cambio de versiones del protocolo de Internet los cuales deben estar al día con su fecha de creación y/o recopilación.

Instrument o de medición

Revisión de documentación disponible en los diferentes medios de divulgación.

Difundir la información obtenida a la comunidad informática costarricense en general para motivarla y orientarla con respecto al cambio.

Variables

- Comunidad informática
- Información

Definición conceptual

Comunidad Informática: conjunto de personas que se dedican a la ciencia de la informática.

Información : comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada.

Definición operativa

Comunidad Informática: conjunto de personas que se desempeñan o dedican profesionalmente a la ciencia de la informática en Costa Rica.

Información : comunicación, conjunto de conocimientos o documentos que permiten ampliar o precisar los que posee la comunidad informática sobre el tema en cuestión.

Instrumento de medición

Recopilación de información disponible sobre el tema.

2. Marco Teórico

El trabajo en redes surgió como resultado de las aplicaciones creadas para las empresas. En el momento en que se escribieron estas aplicaciones, las empresas poseían computadores que eran dispositivos independientes y cada uno operaba de forma individual, independientemente de los demás computadores. Muy pronto se puso de manifiesto que esta no era una forma eficiente ni rentable para operar en el medio empresarial. Las empresas necesitaban una solución que resolviera con éxito las tres preguntas siguientes:

1. Cómo evitar la duplicación de equipos informáticos y de otros recursos
2. Cómo comunicarse con eficiencia
3. Cómo configurar y administrar una red

Las empresas se dieron cuenta de que podrían ahorrar mucho dinero y aumentar la productividad con la tecnología de redes. Empezaron agregando redes y expandiendo las existentes casi tan rápidamente como se producía la introducción de nuevas tecnologías y productos de red. Como resultado, a principios de los 80, se produjo una tremenda expansión del trabajo entre redes y sin embargo, su temprano desarrollo resultaba caótico en varios aspectos.

A mediados de la década del 80 comenzaron a presentarse los primeros problemas emergentes de este crecimiento desordenado. Muchas de las tecnologías de red que habían emergido se habían creado con una variedad de implementaciones de hardware y software distintas. Por lo tanto, muchas de las nuevas tecnologías no eran compatibles entre sí. Se tornó cada vez más difícil la comunicación entre redes que usaban distintas especificaciones.

Una de las primeras soluciones a estos problemas fue la creación de redes de área local (LAN). Como eran capaces de conectar todas las estaciones de trabajo, dispositivos periféricos, terminales y otros dispositivos ubicados dentro de un mismo edificio,

permitieron que las empresas utilizaran la tecnología informática para compartir de manera eficiente archivos e impresoras.

A medida que el uso de los computadores en las empresas aumentaba, pronto resultó obvio que incluso las LAN no eran suficientes. En un sistema de LAN, cada departamento o empresa era una especie de isla electrónica.

Lo que se necesitaba era una forma de que la información se pudiera transferir rápidamente y con eficiencia, no solamente dentro de una misma empresa sino de una empresa a otra. Entonces, la solución fue la creación de redes de área metropolitana (MAN) y redes de área amplia (WAN). Como las WAN podían conectar redes de usuarios dentro de áreas geográficas extensas, permitieron que las empresas se comunicaran entre sí a través de grandes distancias.

Para facilitar su estudio, la mayoría de las redes de datos se han clasificado en redes de área local (LAN) o de área amplia (WAN). Las LAN generalmente se encuentran en su totalidad dentro del mismo edificio o grupo de edificios y manejan las comunicaciones entre las oficinas. Las WAN cubren un área geográfica más extensa y conectan ciudades y países.

A su vez, el proceso de comunicación entre equipos en el principio se tornaba difícil debido a problemas de interoperabilidad ya que cada empresa utilizaba los medios a su disposición para comunicar sus equipos por lo que fue necesario crear un modelo "estándar " de interconexión de redes el cual es conocido como OSI ("Open System Interconnection" Modelo de interconexión de sistemas abiertos) el cual se ha dividido en 7 capas o subprocesos. Dentro del modelo OSI, la capa de red (capa 3) se ocupa de la navegación de los datos o paquetes a través de la red. La función de la capa de red es encontrar la mejor ruta hacia su destino. Los dispositivos utilizan el esquema de direccionamiento de la capa de red (direccionamiento IP) para determinar el destino de los datos a medida que se desplazan a través de la red o redes.

La dirección de red (IP) ayuda al router (enrutador) a identificar una ruta dentro de la nube de red (conjunto de redes). El router utiliza la dirección de red para identificar la red destino de un paquete dentro de la red, una vez que el paquete llega a la red

deseada se vuelve a enrutar dentro de ella hasta llegar a su destino final el cual puede ser por ejemplo, una computadora específica.

Sin el direccionamiento de la capa de red, no se puede producir el enrutamiento y por ello la comunicación entre redes. Los routers requieren direcciones de red para garantizar el envío correcto de los paquetes mediante una estructura jerárquica. Si no existiera alguna estructura de direccionamiento jerárquico, los paquetes no podrían viajar a través de una red. De la misma manera, si no existiera alguna estructura jerárquica para los números telefónicos, las direcciones postales o los sistemas de transporte, no se podría realizar la entrega correcta de mercaderías y servicios. Los protocolos que no tienen capa de red sólo se pueden usar en redes internas pequeñas. Estos protocolos normalmente sólo usan un nombre (por ej. , dirección MAC) para identificar el computador en una red. El problema con este sistema es que a medida que la red aumenta de tamaño, se torna cada vez más difícil organizar todos los nombres como, por ejemplo, asegurarse de que dos computadores no utilicen el mismo.
Los protocolos que soportan la capa de red usan una técnica de identificación que garantiza que haya un identificador exclusivo. ¿Cómo se diferencia este identificador de una dirección MAC, que también es exclusiva? Las direcciones MAC usan un esquema de direccionamiento plano que hace que sea difícil ubicar los dispositivos en otras redes. Las direcciones de capa de red utilizan un esquema de direccionamiento jerárquico que permite la existencia de direcciones exclusivas más allá de los límites de una red, junto con un método para encontrar una ruta por la cual la información viaje a través de las redes.

Los esquemas de direccionamiento jerárquico permiten que la información viaje por una red, y son también un método para detectar el destino de modo eficiente. La red telefónica es un ejemplo del uso del direccionamiento jerárquico. El sistema telefónico utiliza un código de área que designa un área geográfica como primera parte de la llamada (salto). Los tres dígitos siguientes representan el intercambio con la central local (segundo salto). Los últimos dígitos representan el número telefónico destino individual (que, por supuesto, constituye el último salto).

Los dispositivos de red necesitan un esquema de direccionamiento que les permita enviar paquetes de datos a través de el Internetwork (un conjunto de redes formado por múltiples segmentos que usan el mismo tipo de direccionamiento). Hay varios protocolos de capa de red con distintos esquemas de direccionamiento que permiten que los dispositivos envíen datos a través de una Internetwork.

Este identificador exclusivo necesario para la comunicación entre redes se encuentra dentro del Protocolo Internet (IP); es un protocolo enrutable que funciona en la capa de red del modelo OSI(Capa 3) y la capa Internet del modelo TCP/IP (modelo en el que se basa el Internet). IP suministra envío y direccionamiento de paquetes para el origen y destino. El IP no orientado a conexión, que funciona junto a TCP orientado a conexión, forman los estándares de protocolos ideales para el Internet.
Como IP es un servicio no orientado a conexión, no es confiable y no garantiza la entrega de datos o el orden en el que se envían. Sin embargo, a diferencia de los protocolos orientados a conexión, como TCP o HTTP, que pueden ser lentos para enviar paquetes, IP ofrece la entrega rápida de los datos. Al combinarse el IP con el TCP se proporciona direccionamiento y entrega confiable de los paquetes en Internet.

La dirección IP contiene la información necesaria para enrutar un paquete a través de la red. Cada dirección origen y destino contiene una dirección de 32 bits. El campo de dirección origen contiene la dirección IP del dispositivo que envía el paquete. El campo destino contiene la dirección IP del dispositivo que recibe el paquete

Las direcciones IP se expresan como números de notación decimal: se dividen los 32 bits de la dirección en cuatro octetos (un octeto es un grupo de 8 bits).ej.: (11000000.10101000.11110000.00001110 ó "192.168.240.14 en decimal")

Hay tres clases de direcciones IP que una organización puede recibir de parte del Registro Estadounidense de Números de Internet (ARIN) (o por el proveedor de servicios de Internet de la organización, el cual en todo caso las obtenía del ARIN): Clase A, B y C. En la actualidad, ARIN reserva las direcciones de Clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de

gran envergadura como, por ejemplo, Hewlett Packard) y las direcciones de Clase B para las medianas empresas. Se otorgan direcciones de Clase C para todos los demás solicitantes.

De esta manera, la asignación de direcciones comenzó a hacerse de manera centralizada por un único centro de registro (ARIN) satisfaciendo casi todas las solicitudes sin necesidad de mayor trámite. Este modelo de asignación de direcciones, cuando el Internet comenzó a crecer de forma espectacular, trajo algunas de las siguientes problemáticas:

- Escala

  Cada máquina presente en la red dispone de una dirección IP de 32 bits. Ello supone más de cuatro mil millones de máquinas diferentes. Esa cifra, no obstante, es muy engañosa. El número asignado a un ordenador no es arbitrario, sino que depende de una estructura más o menos jerárquica (en especial, pertenece a una red), lo cual ocasiona que se desperdicie una enorme cantidad de direcciones. La cuestión es que en 1.993 fue claro que con el ritmo de crecimiento sostenido de Internet hasta aquel momento (exponencial), el agotamiento del espacio de direcciones era casi inminente.

- Enrutado

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

- Multiprotocolo

  Cada vez resulta más necesaria la convivencia de diversas familias de protocolos: IP, OSI, IPX. Se necesitan mecanismos que permitan abstraer al usuario de la tecnología subyacente para permitir que concentre su atención en los aspectos realmente importantes de su trabajo. Se tiende, pues, hacia una red orientada a aplicaciones, que es con lo que el usuario interacciona, más que una red orientada a protocolos (como hasta el momento) [RFC1560].

- Seguridad

  El mundo IPv4 es el mundo académico, científico, técnico y de investigación. Un ambiente en general que podría calificarse como "amigable", desde el punto de vista de la gestión y la seguridad en la red. Con la aparición de servicios comerciales y la conexión de numerosísimas empresas, el enorme incremento en el número de usuarios y su distribución por todo el planeta, y la cantidad, cada vez mayor, de sistemas que necesitan de Internet para su correcto funcionamiento, es urgente definir unos mecanismos de seguridad a nivel de red. Son necesarios esquemas de autentificación y privacidad, tanto para proteger a los usuarios en sí como la misma integridad de la red ante ataques malintencionados o errores [RFC1281] [RFC1636] [RFC1828..1829].

- Tiempo Real

  IPv4 define una red pura orientada a datagramas y, como tal, no existe el concepto de reserva de recursos. Cada datagrama debe competir con los demás y el tiempo de tránsito en la red es muy variable y sujeto a congestión. A pesar de que en la cabecera IP hay un campo destinado a fijar, entre otras cosas, la prioridad del datagrama [RFC1349] [RFC1455], en la práctica ello no supone ninguna garantía. Se necesita una extensión que posibilite el envío de tráfico de

tiempo real, y así poder hacer frente a las nuevas demandas en este campo [RFC1667].

- Tarificación

  Con una red cada día más orientada hacia el mundo comercial hace falta dotar al sistema de mecanismos que posibiliten el análisis detallado del tráfico, tanto por motivos de facturación como para poder dimensionar los recursos de forma apropiada [RFC1272] [RFC1672].

- Comunicaciones Móviles

  El campo de las comunicaciones móviles está en auge, y aún lo estará más en un futuro inmediato. Se necesita una nueva arquitectura con mayor flexibilidad topológica, capaz de afrontar el reto que supone la movilidad de sus usuarios. La seguridad de las comunicaciones en este tipo de sistemas, se ve además, especialmente comprometida [RFC1674] [RFC1688].

- Facilidad de Gestión

  Con el volumen actual de usuarios y su crecimiento estimado, resulta más que obvio que la gestión de la red va a ser una tarea ardua. Es preciso que la nueva arquitectura facilite al máximo esta tarea. Un ejemplo de ello sería la autoconfiguración de los equipos al conectarlos a la red [RFC1541].

- Política de enrutado

  Tradicionalmente los datagramas se han encaminado atendiendo a criterios técnicos tales como el minimizar el número de saltos por efectuar y el tiempo de permanencia en la red. Lo ideal es que la red pertenezca a una única organización, pero en el nuevo entorno económico en el que diferentes proveedores compiten por el mercado, las cosas no son tan simples. Es

imprescindible que la fuente pueda definir por cuales redes desea que pasen sus datagramas, atendiendo a criterios de fiabilidad, costo, retardo y privacidad. [RFC1674..1675].

Por tanto, nos encontramos ante un grave problema en el cual destaca el agotamiento de direcciones y colapso de routers debido a la explosión de rutas. En una situación en la que la población conectada a la red se duplicaba (en términos de equipos y redes conectadas) en periodos que oscilaban en torno a los 6 meses había que tomar medidas urgentes, y he aquí algunas:

- Imposición de políticas restrictivas de asignación de direcciones por parte de los centros de registros (ya descentralizados del primitivo NIC).
- Modificación de los protocolos exteriores de enrutamiento para soportar prefijos de red variables.
- Para entender bien el problema hay que tener en cuenta que el periodo en el que los fabricantes duplican la capacidad de proceso de sus equipos y la de sus memorias es de aproximadamente dos años. La capacidad de los routers que deben mantener en sus tablas una información completa o full-routing sobre la topología de el Internet "equipos conectados a los backbones principales o de dominios conectados a múltiples proveedores" se habría hoy superado, con el colapso consiguiente de el Internet, si el método de asignación de prefijos variables no hubiese sido puesto en funcionamiento a principios de 1994. En este momento existen más de 60.000 redes conectadas mientras que los equipos que soportan full-routing manejan alrededor de 30.000 prefijos.

De forma repetida vemos como se achaca a el Internet el ser un medio de comunicación inseguro. Este es un tema con muchos ángulos y que debe ser examinado en cada una de sus partes. Dado el carácter puramente académico de el Internet en su comienzo, los asuntos relativos a la seguridad fueron, como desgraciadamente suele ocurrir en la práctica, relegados a posterior estudio hasta que los primeros ataques globales hacen sonar la alarma y empieza a producirse un notable esfuerzo en incorporar mecanismos de seguridad a las aplicaciones existentes, el

problema de seguridad en el nivel de red sigue sin ser tomado en cuenta y comienza a producirse una serie de ataques cada vez más sofisticados basados en la suplantación de la identidad de máquinas conectadas a la red, dando la posibilidad de violar un acceso prohibido o de escudriñar (o desviar) la información a intrusos. Como respuesta surgieron mecanismos de barrera como los cortafuegos, pero los protocolos siguen sin incorporar medidas específicas de seguridad.

Pero esto es sólo una parte del problema. La seguridad integral comprende servicios tanto de confidencialidad como de autentificación, integridad y no rechazo para los que se requieren técnicas de encriptación que están sujetas a diferentes normativas de exportación y uso en determinados países, lo que hace complicado su utilización generalizada en un medio que se tiene por libre y homogéneo (en cuanto al tipo de protocolos y aplicaciones empleados). Se corre el peligro de fracturar el Internet en zonas donde se pueda intercambiar información de forma segura y otras en que no, bien por considerarse tecnología de uso militar, bien por el derecho que se guardan algunos gobiernos a poder intervenir -e interpretar- las comunicaciones de sus ciudadanos.

En otro orden de cosas, estamos asistiendo al nacimiento de servicios de transmisión de información en tiempo real dentro de el Internet. Ejemplos de ello son las aplicaciones para comunicaciones de voz a través de la red, red virtual superpuesta a el Internet basada en el concepto de IP Multicast. Un defecto claro de IPv4 es la falta de caracterización de los distintos flujos de información que viajan por la red, sujeta más la redundancia de un mecanismo corrector de transporte que a una transmisión de voz en tiempo real en la que la pérdida de un número significativo de paquetes puede alterar o incluso imposibilitar la interpretación de la información. La aparición de este tipo de servicios en la era de las autopistas de la información presenta una clara limitación del uso de el Internet tal y como la concebimos actualmente.

En cualquier caso, hay que entender que tanto la asignación de prefijos de longitud variables como las políticas restrictivas de asignación de direcciones son sólo medidas temporales, dirigidas a afrontar problemas concretos y que no resuelven (en algunos casos hasta agravan) los problemas crónicos detectados en Internet en gran parte debidos a su tremendo éxito. Así, se han llegado a plantear iniciativas como la

devolución de direcciones, la obligatoriedad de cambiarlas al modificar el proveedor, su asignación dinámica, el uso de traductores de direcciones (NAT) que transformen un espacio privado de direcciones en otro perteneciente al proveedor, o incluso el cobrar una cantidad elevada por cada prefijo (no perteneciente al espacio del proveedor) que un cliente desee que su proveedor anuncie.

Aunque los investigadores desarrollaron soluciones provisionales para posponer el "Día del Juicio Final", hoy está ocurriendo otra vez lo mismo: todas las direcciones IP actuales se agotarán en algún momento entre el 2005 y el 2010 si la tasa de crecimiento de Internet continúa.

Para remediar estos males, los cuerpos técnicos de el Internet impulsaron un debate bajo el lema de IP Next Generation (IPng) que ha culminado con la especificación de un nuevo protocolo IP, sucesor del actual IPv4, y conocido formalmente como la versión 6 del Protocolo Internet o IPv6.

Aunque mucho se ha escrito sobre este tema aún no se ha elaborado una guía que informe mejor al profesional en informática. Esto provoca la necesidad de que la comunidad informática cuente con un compendio de información que le facilite su comprensión y el impacto que tendrá a nivel mundial y le ayude a dar ese paso que es cada vez más inminente y así poder explotarlo de una manera positiva.

De aquí se obtiene el objetivo principal de esta investigación: "Recopilar y brindar información sobre la nueva generación del protocolo de Internet (IPv6)"; dirigido a la comunidad informática costarricense en el cual se verán aspectos claves del proceso como el Hardware y Software actual y sus tendencias. Esto es importante ya que ubica en cuando a la dirección tecnológica que se está dando, en este sentido, en forma separada del Hardware y Software de comunicaciones; lo cual es imprescindible ya que los equipos de comunicaciones son la base o centro de las redes de comunicaciones actuales. El Recurso Humano es uno de los puntos más importantes ya que se encarga de planear, manejar, controlar y ejecutar el proceso. También las empresas deben informarse acerca del Costo/Beneficio; ya que este proyecto repercute directamente en las empresas que se dedican a cualquier tipo de actividad; para estas es importante medir el impacto costo/beneficio de un proyecto de tal envergadura. Además del Costo/Beneficio se debe tomar en cuenta las Implicaciones Administrativas;

ya que representan directamente al personal gerencial o administrativo de las empresas, el tipo de reto al que se enfrentan y las implicaciones que conlleva.

De esta manera, se pretende cubrir todas estas variables y con ello preparar a la comunidad informática costarricense sobre el acontecimiento tan grande que están por enfrentar; generando una documentación actualizada y difundiéndola entre esta población; así quedan integrados al nuevo Internet, el cual incluye un número in-imaginado de personas y servicios y que será sin duda alguna la forma de comunicación más importante del siglo XXI.

3. Metodología

3.1 Métodos de investigación

Por medio de los métodos de investigación se muestra la forma sistemática en que se obtuvieron los datos y la información requerida para la propuesta. Para Jaime Arellano (1987):

> "Método en general, es un conjunto de procedimientos sistemáticamente diseñados para lograr un objetivo".

Existen varios modelos metodológicos que pueden ser utilizados para fundamentar la recopilación de datos para la investigación que dependen de sus características y circunstancias; así como el tipo de estudio.

Según otros investigadores, si una vez realizada la revisión de la literatura se ha decidido que la investigación vale la pena y que se debe llevar a cabo, el siguiente paso consiste en elegir el tipo de estudio que se efectuará; de acuerdo con el tipo de estudio que se trate, variará la estrategia de investigación.

Toda investigación tiene como propósito dar respuesta a los problemas por medio de la recopilación lógica y ordenada de los datos, la cual se efectúa de diversas maneras entre las que están: Investigación Exploratoria, Investigación Descriptiva, Investigación Aplicada.

Investigación Exploratoria

Consiste en la preparación del campo de acción en el cual se efectúa el estudio, trata de detectar mediante distintos medios los detalles por los que está rodeado el problema y las fuentes de información que den soporte a la investigación.

Permite observar y descubrir las variables que rodean la situación, originando una familiarización con el estudio. Según Roberto Fernández Sampieri (1996) :

> "Los estudios exploratorios se efectúan, normalmente, cuando el objetivo es examinar un tema o problema de investigación poco estudiado o q ue no ha sido abordado antes. Es decir, cuando la revisión de la literatura reveló que únicamente hay guías no investigadas e ideas vagamente relacionadas con el problema de estudio....
> Los estudios exploratorios nos sirven para aumentar el grado de familiaridad con los fenómenos relativamente desconocidos, obtener información sobre la posibilidad de llevar a cabo una investigación más completa sobre un contexto particular de la vida real ."

En esta investigación, la metodología exploratoria se utiliza durante todo el proceso que lleva la creación de este documento. Esta metodología permite el conocimiento y la familiarización con el contexto en el cual se realiza la investigación " IPV6 ". La observación acompañada con el análisis de los datos y la búsqueda de la literatura estuvieron presentes desde el momento en que se decidió realizar el proyecto.

Investigación Descriptiva

La investigación descriptiva no se limita solamente a la recolección y tabulación de los datos, sino que analiza e interpreta su significado con el propósito de derivar conclusiones significativas. Para John W. Best (1987):

"La Investigación Descriptiva se refiere minuciosamente e interpreta lo que es...
A veces, la Investigación Descriptiva concierne a cómo lo que es o lo que existe se relaciona con algún hecho precedente, que haya influido o afectado una condición de hechos presentes."

Esta investigación además de recolectar dados por distintos medios y su tabulación; interpreta su significado. Esto impacta directamente sobre el curso de la investigación; de manera que dependiendo de los resultados obtenidos con los datos; especialmente la encuesta dirigida a la comunidad informática se muestra cuáles son los sub-temas en que debemos enfatizar o en cuales ser más superficiales o por qué no nos podría introducir en nuevos sub-temas.

Investigación Aplicada

La Investigación Tecnológica Aplicada utiliza los conocimientos de la investigación básica o pura para ponerlos al servicio en la práctica. Guarda íntima relación con la Investigación Descriptiva, ya que depende de los descubrimientos y avances de la investigación básica y se enriquece con ellos.

Para John W. Best (1987);

" La investigación básica o pura es la que se realiza con el propósito de acrecentar los conocimientos teóric os para el progreso de una determinada ciencia, sin interesarse directamente en su posible aplicación o consecuencias prácticas, es más formal y persigue propósitos teóricos en el sentido de aumentar el acervo de conocimientos de una determinada teoría.
Por su parte, la investigación aplicada guarda íntima relación con la anterior, pues depende de los descubrimientos y avances de la investigación básica y se enriquece con ellos. Se trata de

> investigaciones que se caracterizan por su interés en la aplicación , utilización y consecuencias prácticas de los conocimientos".

Para efectos de esta investigación no se pretende aplicar directamente los conocimientos adquiridos sino más bien formar una base de información y conocimiento para la comunidad informática costarricense y de esta manera permitir que la aplique a su área de trabajo convirtiéndola así en una investigación aplicada.

3.2 Sujetos de Investigación

Son todas aquellas personas o individuos que por su experiencia o relación con una situación dada, están en capacidad de dar información valiosa con respecto al tema investigado, con el fin de encontrar una solución eficiente al problema.

En el caso de nuestra investigación, el principal sujeto lo constituye la comunidad informática costarricense.

3.3 Población y Muestra

Con cierta frecuencia se escuchan afirmaciones como: "todas las mujeres son..." o " todos los hombres son..." las cuales se sustentan en una de dos situaciones:

a) En lo mucho o poco que la persona ha oído o leído respecto al grupo en mención.
b) En lo mucho o poco que haya experimentado en su trato con cierto número de miembros del grupo en cuestión.

Pero definitivamente, es seguro que no puede sostenerse que estas afirmaciones se sustentan en una experiencia directa con todos los hombres o todas las mujeres que existan o hayan o vayan a existir. Más bien se refiere a un subconjunto, muchas veces limitado de estas personas, las cuales representan de manera apropiada a todas las demás.

En el caso de la afirmación "todos los hombres", tenemos una declaración que se refiere a cierta unidad de análisis o de observación en particular -hombre-. De todo lo que existe, la afirmación se refiere a quienes comparten las características propias de un hombre. Una vez que se determina la unidad de observación, se está en condiciones de identificar la población o universo: a todas las posibles unidades de observación.

En el caso de una buena parte de las investigaciones, no es posible tener contacto y observar a todas las unidades de análisis posibles, por lo que es

necesario seleccionar un subconjunto que en efecto represente de manera apropiada a toda la población.

El Muestreo

Muestreo es tomar una porción de una población como subconjunto representativo. Para que la muestra, al menos teóricamente, sea representativa de la población, debe seleccionarse siguiendo un procedimiento que permita a cualquiera de todas las posibles muestras del mismo tamaño contenidas en la población, tener igual oportunidad de ser seleccionada. Este procedimiento es el muestreo aleatorio.

Muestras Aleatorio o al azar

Se le da a cada uno de los elementos de la población una probabilidad conocida de ser incluido en la muestra. Un caso particular es aquél en que a todos los elementos se les da la misma probabilidad; este procedimiento recibe el nombre de muestreo simple al azar.

Muestreo Intencional

Se aplica utilizando el juicio de una persona con experiencia y conocimiento con respecto a la población que estudia.

Muestras por Conveniencia

Se aplica escogiendo las unidades o elementos que están disponibles o que son más fáciles de conseguir.

Cálculo de la muestra

Cuando se hace una muestra, uno debe preguntarse; dado que una población es N ; ¿cuál es el menor número de unidades muestrales que es necesario para conformar una muestra n ?; que asegure un error estándar de 0.030[*]. Entonces se tiene;

[*] Un error estándar de 0.030 indica el grado de confianza o certeza que se tiene en la muestra seleccionada; esto tratando de que el error sea lo más aceptable deseado sin que esto obligue a evaluar a toda la población ya que ambas razones son inversamente proporcionales. Es decir en

Planteo

N = tamaño de la población de 2285 informáticos.

Y = valor promedio de la variable = 1; un informático" en este caso sólo un valor puede tener.".

se = error estándar = 0.030; determinado por el investigador.

V^2= Varianza de la población.

$S^{2\,=}$ Varianza de la muestra expresada como la probabilidad de ocurrencia de y.

Operación

$$s' = s^2 / v^2$$
$$s^2 = p(1-p) = 0.9(1-0.9) = 0.09$$
$$V = (0.30)^2 = 0.0009$$
$$n' = 0.09 / 0.0009 = 100$$
$$n = n'/(1+n'/N) = 100/(1+100/2285) = 95.8071279$$

Respuesta

Para la investigación se necesitará una muestra de 95.8071279 informáticos.

Para la presente investigación se definió como sujeto de estudio la comunidad informática costarricense que labora en la provincia de San José y que esté formalmente inscrita en el Colegio de Profesionales en Informática de Costa Rica (CPIC). De ello se obtiene que existan actualmente (a enero del 2004) 2285 socios activos, de los cuales interesa entrevistar 96. Esto se realizará por una muestra por conveniencia como ya se indicó en la provincia de San José ya que

este caso de cada 100 casos, 3 eventualmente no cumplirían con los requerimientos; lo que es muy aceptable.

es casi imposible debido a su disponibilidad física entrevistar a toda la población que esta dispersa por todo el país y por el tipo de estudio no interfiere con el este. Se considera que esta muestra es lo suficientemente representativa ya que debido al tamaño de la población es casi imposible físicamente cubrirla, además la aplicación a toda la población resultaría demasiado costosa y tomaría tanto tiempo que los datos obtenidos resultarían obsoletos en el momento de la culminación del presente estudio. Además, los resultados que arrojaría una muestra bien seleccionada y de tamaño razonable serían suficientemente precisos para los fines prácticos que se persigue con los datos. Una muestra es representativa cuando contiene aproximadamente la misma proporción de sujetos pertenecientes a los distintos grupos (cronológicos, sociales y técnicos) que la población completa de donde se tomó, lo que permitiría hacer extensivas las conclusiones a toda la población. Por lo tanto, se puede decir que la muestra es representativa en este caso de estudio.

3.4 Fuentes de Información

Las fuentes de información se dividen en primarias y secundarias.

Fuentes primarias

> "Aquellas fuentes que contienen información nueva u original y cuya disposición no sigue, habitualmente, ningún esquema predeter minado. Se accede a ellas directamente o por las fuentes de información secundarias. Ejemplos: revista científica, literatura gris, actas."

Fuentes secundarias

> "Aquellas que contienen material ya conocido, pero organizado según un esquema determinado. La información que contiene referencia a documentos primarios. Son el resultado de aplicar las técnicas de análisis documental sobre las fuentes primarias y de la extracción, condensación u otro tipo de reorganización de la información que aquéllas contienen, a fin de hacerla accesible a los usuarios. Ejemplos: Revistas de resúmenes, índices."

En esta investigación se usarán fuentes primarias y secundarias. También existen las terciarias, las cuales se usarán sólo para complementar la información obtenida de una fuente secundaria o primaria con el fin de explicar lo más posible cada sub-tema que se trate en esta investigación.

Se utilizarán fuentes primarias para investigar los antecedentes, historia, compatibilidad, etc. de las versiones del protocolo de Internet.

Las fuentes secundarias se usarán para complementar la información obtenida de las fuentes primarias, y así analizar información de más peso y seleccionar lo que más interesa destacar de cada sub-tema sin perder la objetividad.

Las fuentes terciarias serán utilizadas en cualquier momento como complemento de una fuente primaria o secundaria de información.

3.5 Instrumentos

Jaime Arellano(1987), indica, que toda investigación necesita de un método para lograr su objetivo; refiriéndose a método como una estrategia general que responde a la pregunta " cómo se hace la recolección "; señala además que un método puede perfectamente no recurrir a ningún instrumento, o recurrir, según las circunstancias a diferentes instrumentos.

El autor se refiere a los instrumentos como los ingredientes del método (herramientas) que responden a la pregunta " Con qué se hace... ".

Entre la clasificación de los instrumentos se tienen:

Instrumentos de simple recolección: Son utilizados para recoger la información en forma organizada, útil a los propósitos de la investigación (observación, cuestionarios, entrevistas.)

Instrumentos de medición: Son utilizados para medir capacidades, rasgos, actividades estudiadas (normalmente de modo indirecto) Ejemplos de este tipo de instrumentos lo son el test, los inventarios de personalidades y las escalas de actitudes.

La Observación

Según Marcelo Blanc (1984), la observación consiste en:

"... la aproximación directa mediante los sentidos y la presencia física del investigador a los hechos y/o fenómenos que se desean estudiar."

Marcelo Blanc indica; " que la observación es empleada en forma espontánea en la vida diaria; pero cuando es utilizada para investigar se caracteriza por la selectividad; trata de seleccionar los hechos o datos relevantes que sirvan para explicar el tema a ser investigado ".

De acuerdo con los medios utilizados o el lugar donde se realiza, la observación puede ser:

Observación no estructurada: Consiste en reconocer y anotar los hechos sin la ayuda de medios técnicos especiales.

Observación estructurada: recurre al empleo de instrumentos o guías para la recopilación de datos, estableciendo de antemano los aspectos por estudiarse (anotaciones, cuadros estadísticos, listados, grabadoras.)

Observación participante: es donde el observador se presenta como un espectador sin intervenir directamente en el proceso observado.

En esta investigación se utiliza la investigación no estructurada ya que se recolecta la información sin el uso de medios técnicos específicos ni establecidos de antemano; sino más bien las herramientas y los métodos se van aplicando conforme se va desarrollando la investigación. Además se utiliza la observación participante ya el observador "investigador" se presenta como un espectador en el proceso siempre recopilando y documentando la información pero sin intervenir o desviar directamente el proceso observado.

El Cuestionario

El Cuestionario es un instrumento de investigación. Se utiliza de un modo preferente en el desarrollo de una investigación en el campo de las ciencias sociales: es una técnica ampliamente aplicada en la investigación cualitativa.

No obstante, su construcción, aplicación y tabulación posee un alto grado científico y objetivo. Elaborar un cuestionario válido no es una cuestión fácil; implica controlar una serie de variables.

El Cuestionario es un medio útil y eficaz para recoger información en un tiempo relativamente breve.

En su construcción pueden considerarse preguntas cerradas, abiertas o mixtas.

Características

- Es un procedimiento de investigación.
- Es una entrevista altamente estructurada.
- Un cuestionario consiste en un conjunto de preguntas respecto a una o más variables por medir.
- Presenta la ventaja de requerir relativamente poco tiempo para reunir información sobre grupos numerosos.
- El sujeto que responde proporciona por escrito información sobre sí mismo o sobre un tema dado.
- Presenta la desventaja de que quien contesta responda escondiendo la verdad o produciendo notables alteraciones en ella. Además, la uniformidad de los resultados puede ser aparente, pues una misma palabra puede ser interpretada en forma diferente por personas distintas, o ser comprensibles para algunas y no para otras. Por otro lado, las respuestas pueden ser poco claras o incompletas, haciendo muy difícil la tabulación.

Cuestionario Restringido o Cerrado

- Es aquel que solicita respuestas breves, específicas y delimitadas.
- Para poder formular preguntas cerradas es necesario anticipar las posibles alternativas de respuestas.
- Estas respuestas piden ser contestadas con:

a)Dos opciones de respuestas (respuestas dicotómicas): Sí o No.

b)Varias opciones de respuestas: donde se señala uno o más ítemes (opción o categoría) en una lista de respuestas sugeridas. Como no es posible prever todas las posibles respuestas, conviene agregar la categoría Otros o Ninguna de las Anteriores, según sea el caso. En otras ocasiones, el encuestado tiene que jerarquizar opciones o asignar un puntaje a una o diversas cuestiones.

- Ventajas
  - Requiere de un menor esfuerzo por parte de los encuestados.
  - Limitan las respuestas de la muestra.
  - Es fácil de llenar.
  - Mantiene al sujeto en el tema.
  - Es relativamente objetivo.
  - Es fácil de clasificar y analizar.

Cuestionario No Restringido o Abierto

- Las preguntas abiertas no delimitan de antemano las alternativas de respuesta.
- Las preguntas abiertas son particularmente útiles cuando no tenemos información sobre las posibles respuestas de las personas o cuando esta información es insuficiente.
- Es aquel que solicita una respuesta libre.
- Esta respuesta es redactada por el propio sujeto.
- Proporciona respuestas de mayor profundidad.
- Es de difícil tabulación, resumen e interpretación.

Cuestionario Mixto

- Es aquél que considera en su construcción tanto preguntas cerradas como abiertas.

Requerimientos para la construcción de un buen Cuestionario

- Hacer una lista de aspectos (variables) que se consideran importantes de incluir.
- Determinar el propósito del cuestionario. Se refiere a un tema significativo.
- Señalar el título del proyecto, del aspecto o tema a que se refiere, y una breve indicación de su contenido. Las instrucciones deben ser claras y completas.
- Especificar algunos datos generales: institución, fecha, nombre del encuestador, entro otros.
- Establecer la mejor secuencia de dichos aspectos o temas.
- Los términos importantes deben estar definidos.
- El cuestionario no ha de ser demasiado largo.
- No es conveniente iniciar el cuestionario con preguntas difíciles o muy directas.
- Escribir un esquema de posibles preguntas pensando lo que se pretende averiguar con cada una de ellas, procediendo posteriormente, si es necesario, a su reubicación, modificación o eliminación. Cada pregunta implica una sola idea. Las preguntas deben ser objetivas, es decir, sin sugerencias hacia lo que se desea como respuesta. En relación con este punto, es conveniente hacerse las siguientes interrogantes:
  - ¿Es necesario o útil hacer esta pregunta?
  - ¿Es demasiado general?
  - ¿Es excesivamente detallada?
  - ¿Debería la pregunta ser subdividida en otras preguntas más pequeñas y ser más concreta, específica?
  - ¿La pregunta se refiere preferentemente a un solo aspecto?
  - ¿Se refiere a un tema sobre el cual las personas encuestadas poseen la información necesaria?
  - ¿Es posible contestarla sin cometer errores?
  - ¿Son las palabras suficientemente simples como para ser comprendidas por el encuestado?
  - ¿Es la estructura de la frase fácil y breve?
  - ¿Son las instrucciones claras y precisas?

- ¿Es necesario clarificarla con alguna ilustración?
- ¿Es posible que tal pregunta incomode al encuestado?
- ¿La pregunta induce la respuesta? ("Las preguntas no pueden apoyarse en instituciones, ideas respaldadas socialmente ni en evidencia comprobada").

- "La elección de tipo de preguntas que contenga el cuestionario depende del grado en que se puedan anticipar las posibles respuestas, los tiempos de que se disponga para codificar y si se quiere una respuesta más precisa o profundizar en alguna cuestión".

J. W. Best , da las siguientes sugerencias en relación con la construcción de cuestionarios:

1. Busca solamente la información que se puede obtener de otras fuentes.
2. Es tan breve como sea posible y sólo lo bastante extenso para obtener los datos esenciales.
3. Tiene un aspecto atractivo.
4. Las instrucciones son claras y completas. Los términos importantes se hallan definidos; cada pregunta implica una sola idea; todas ellas están expresadas tan sencilla y claramente como sea posible, de manera que permite respuestas fáciles, exactas y sin ambigüedad.
5. La importancia del tema al cual se refiere, debe ser expuesta clara y cuidadosamente en el cuestionario. Las personas estarán más dispuestas a responder si saben cómo serán utilizadas sus respuestas.
6. Las preguntas son objetivas, sin sugestiones hacia lo que se desea como respuesta.

7. Las preguntas están presentadas en un orden psicológico correcto, precediendo las de tipo general a las específicas. Deben evitarse las preguntas molestas.
8. Es fácil de clasificar o interpretar.
9. Antes de aplicar un cuestionario a un grupo numeroso, conviene experimentarlo en un grupo reducido de características lo más semejantes a las personas a las que se va a encuestar. Esta aplicación previa tiene por objeto detectar preguntas e instrucciones ambiguas que posteriormente pueden restar validez al instrumento. Es lo que se denomina cuestionario piloto de la prueba.
10. Al elaborar el cuestionario es necesario establecer la forma en que será tabulado e interpretado. Para este objeto, es de gran utilidad la aplicación experimental que permite prever la dispersión que tendrán las respuestas. Una de las formas más sencillas de tabular un cuestionario es construir una tabla de doble entrada, en uno de cuyos ejes se registra a los encuestados o el número de formulario si se aplicó en forma anónima, y en su otro eje se colocan las preguntas o el número que las representa. De este modo es posible obtener rápidamente una visión global de las respuestas dadas por los individuos encuestados.

En esta investigación se utilizará un cuestionario mixto ya que para el tema en cuestión no sería objetivo el aplicar un solo tipo de preguntas; se aplicarán preguntas de respuesta cerrada en ciertos casos y en otros nos es importante conocer la opinión del entrevistado por lo que se utilizarán preguntas abiertas; eso sí para efectos de tabulación de la información se tratará de juntar o buscar similitudes entre estas respuestas abiertas para que los datos obtenidos nos sean significativos a nuestra población y no individualizarlas totalmente. Se crearán primero algunos cuestionarios de prueba los cuales serán aplicados aleatoriamente para así probar su efectividad y crear el cuestionario final que se aplicará a la población en estudio.

4. Análisis de Datos

A continuación se detalla y analizan los datos obtenidos con los instrumentos de investigación, más específicamente con el cuestionario que fue utilizado para esta investigación; el cual se aplicó en forma individual a la muestra obtenida en el capítulo anterior, la cual está compuesta por 98 informáticos, debidamente inscritos en el colegio profesional.

Lo que se busca mediante este análisis es aclarar y especificar el estado del tema de investigación para así saber cuál es la situación actual y tomar esta información como un punto de partida para el desarrollo de la propuesta; dando énfasis a los temas que así lo requieren según los resultados obtenidos. A la vez se explorará los datos obtenidos para darles un enfoque más gráfico y explicativo. Se debe recalcar que es importante analizar profundamente los datos obtenidos, porque solo así se podrán tener conclusiones más verídicas de la situación actual de la comunidad informática costarricense en cuanto al tema de estudio.

Los cuestionarios se aplicaron a los 98 informáticos, la mayoría residentes en la provincia de San José, y colegiados; algunas de las empresas en donde se aplicaron son: Ministerio de Hacienda "División Informática de Aduanas", Dirección General informática del Ministerio de Hacienda; Banca Promérica, Departamento de Soporte Técnico, Funcionarios de informática de Acueductos y Alcantarillados y "Logical Data", entre otros. El cuestionario consistió de 19 preguntas cuyos resultados se analizarán a continuación:

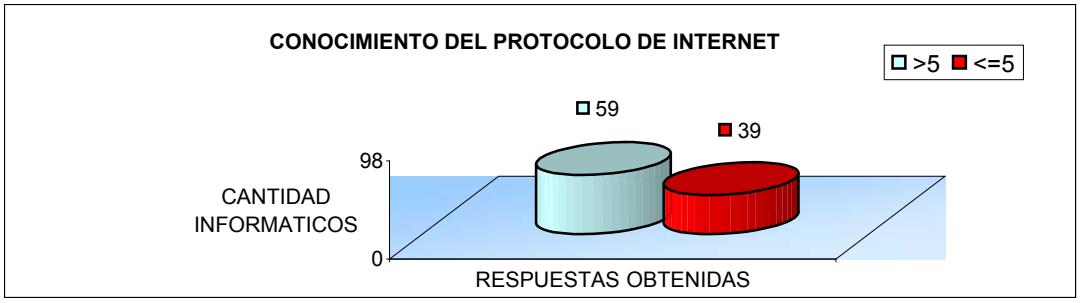
4.1 Análisis específico de los resultados

A continuación se muestran los resultados obtenidos para cada una de las preguntas y el análisis de los datos obtenidos.

1. ¿Cuánto conoce usted acerca del protocolo de Internet "IP"?

Esta pregunta se evaluó con una escala del 1 a 10; el resultado obtenido es el siguiente

Gráfico 1



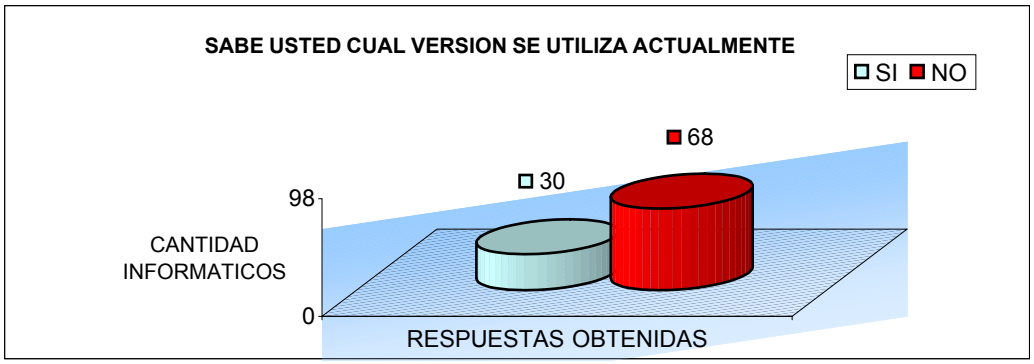
Fuente: Cuestionario aplicado a la población informática costarricense.

El resultado es bastante aceptable. Se nota que los profesionales tienen conocimiento suficiente del protocolo de Internet en general; esto ayuda a que no se deba ocupar gran parte de la investigación en la introducción al tema. Sin embargo, se hará una para cubrir esas 39 personas que no tienen un buen nivel de conocimiento, lo cual dará fundamento para introducirlos al tema del cambio de protocolo.

2. ¿Sabe usted cuál es la versión de "IP" que se utiliza actualmente?

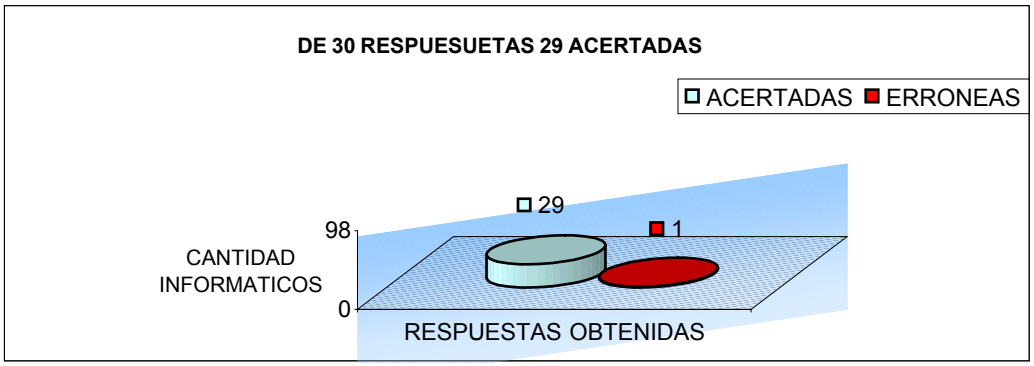
Esta pregunta se evaluó con dos opciones posibles sí y no; sin embargo, si el encuestado respondía que sí, se le preguntaba cuál era la versión actual.

Gráfico 2



Fuente: Cuestionario aplicado a la población informática costarricense.

Gráfico 3



Fuente: Cuestionario aplicado a la población informática costarricense.

Esta respuesta es preocupante, ya que aunque en la anterior 59 personas dicen tener conocimiento suficiente del protocolo de Internet; 68 no saben cuál es la versión actual y al verificar si en realidad lo sabían el total de respuestas correctas disminuye un poco, lo que deja al final un resultado de 29 profesionales de la muestra que sí sabe cual versión se utiliza actualmente. Al tomar en cuenta que este protocolo es "una

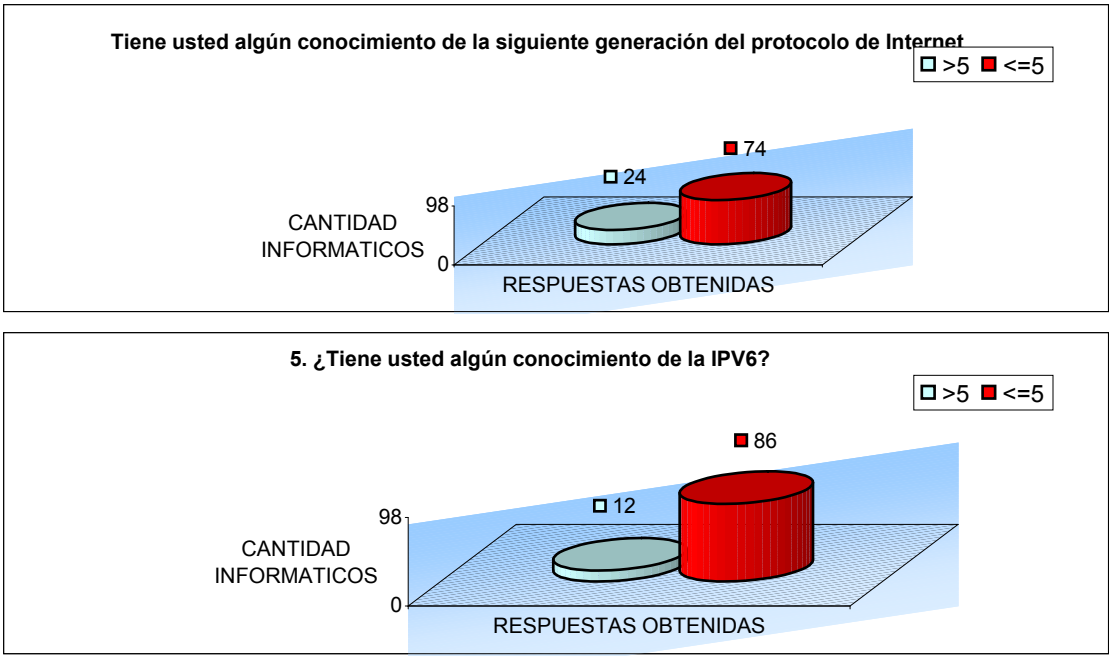
herramienta" del trabajo diario, se deben ampliar los contenidos en cuanto a la versión actual del protocolo de Internet; sus características, fortalezas, debilidades y su estado actual. Esto con el fin de informar a las personas que no poseen el conocimiento así como también reforzar el de las personas que sí lo tienen.

3. ¿Tiene usted algún conocimiento de la siguiente generación del protocolo de Internet?

Esta pregunta va relacionada con la pregunta #5 (¿Tiene usted algún conocimiento de la IPV6?)

Ambas son cruzadas y se evaluaron con una escala del 1 a 10; el resultado obtenido es el siguiente:

Gráfico 4



Fuente: Cuestionario aplicado a la población informática costarricense.

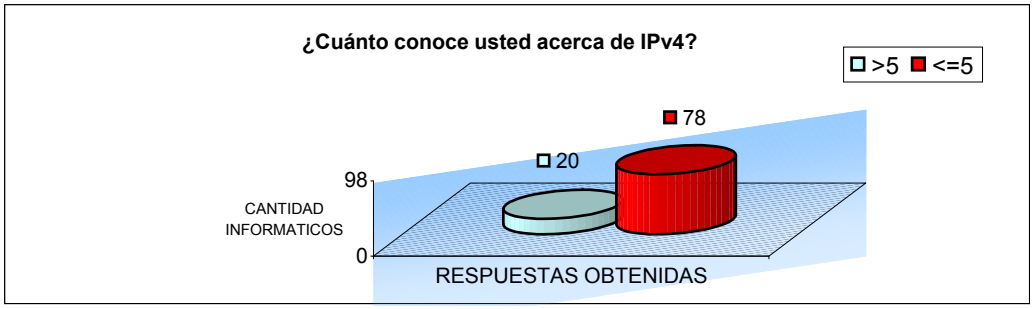
Se tiene un resultado poco aceptable al preguntar el conocimiento sobre la nueva versión del protocolo; tanto es así que con sólo cambiar la pregunta el resultado varió a la mitad de lo antes obtenido; lo cual dice que en realidad el desconocimiento de la versión 6 del protocolo es grande por lo que hay que enfatizar en este tema en la investigación para aclarar e informar adecuadamente a los informáticos sobre el nuevo

protocolo, antecedentes, características, mejoras, cambios en cuanto a la versión 4 (una vez se haya explicado para tener una base de comparación), y algunos pormenores que motivaron al cambio o su actualización del protocolo; que es la intención principal de la elaboración del presente proyecto.

4. ¿Cuánto conoce usted acerca de IPv4?

Esta pregunta se evaluó con una escala del 1 a 10; el resultado obtenido es el siguiente:

Gráfico 6



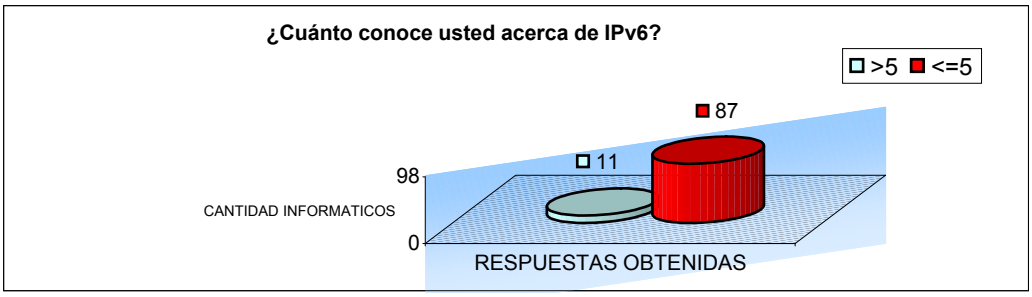
Fuente: Cuestionario aplicado a la población informática costarricense.

Al querer cuantificar el conocimiento de la versión actual del protocolo de Internet, el resultado deja bastante que desear, lo que refuerza lo obtenido en la pregunta dos y dice que es necesario abarcar el tema de la versión actual del protocolo de Internet para así lograr una base necesaria para la introducción y comprensión adecuada de la nueva versión.

5. ¿Cuánto conoce usted acerca de IPv6?

Esta pregunta se evaluó con una escala del 1 a 10; el resultado obtenido es el siguiente:

Gráfico 7



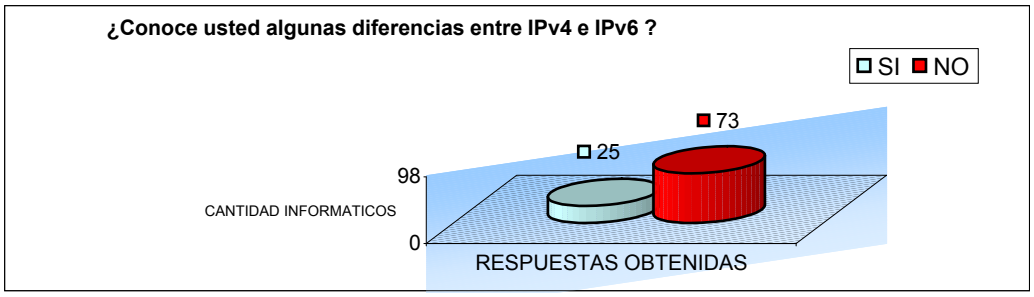
Fuente: Cuestionario aplicado a la población informática costarricense.

Como que su antecesor la versión 6 del protocolo de Internet es aun menos y es necesario en esta investigación plasmar la información necesaria para dotar al profesional costarricense por lo menos de un conocimiento básico que lo introduzca al tema. En nuestro país se le debería dar más importancia como se hizo en el pasado con el cambio de milenio (Y2K); ya que solo así se podrá preparar adecuadamente para enfrentar este importante proceso de cambio. Mediante la presente investigación se pretende sembrar y provocar en la comunidad informática costarricense la inquietud sobre el tema y de esta manera que cada profesional investigue y complemente la información requerida para implementar el cambio en cada organización sin importar su mercado.

6. ¿Conoce usted algunas diferencias entre IPv4 e IPv6 ?

Esta pregunta se evaluó con dos opciones posibles sí y no; sin embargo, si el encuestado respondía que sí se le preguntaba por tres diferencias:

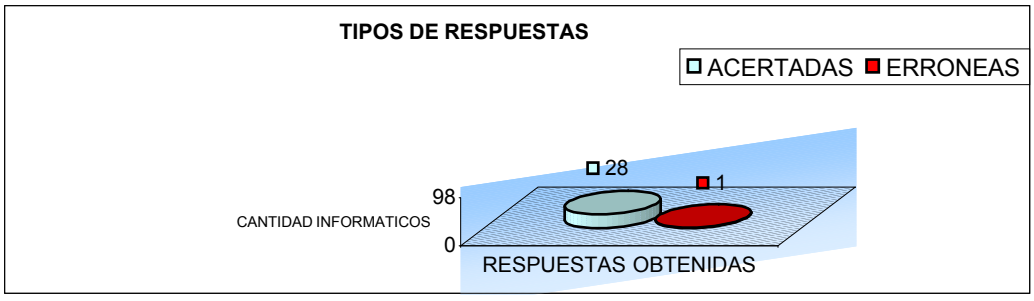
Gráfico 8



Fuente: Cuestionario aplicado a la población informática costarricense.

Es preocupante el resultado pero se debe recordar que para tener conocimiento de la diferencia entre las dos versiones del protocolo hay que tener dominio de ambas; al conocerlas y sus características se va a justificar el cambio; por ello en este documento se pretende informar a la comunidad informática para que comprenda este tema y pueda enfrentar el cambio de versiones.

Gráfico 9



Fuente: Cuestionario aplicado a la población informática costarricense.

Al consultar algunas de las características (a los que dijeron saber algunas) las respuestas fueron favorables; ya que confirmaron saber lo que decían; entre las respuestas obtenidas las más reiteradas fueron:

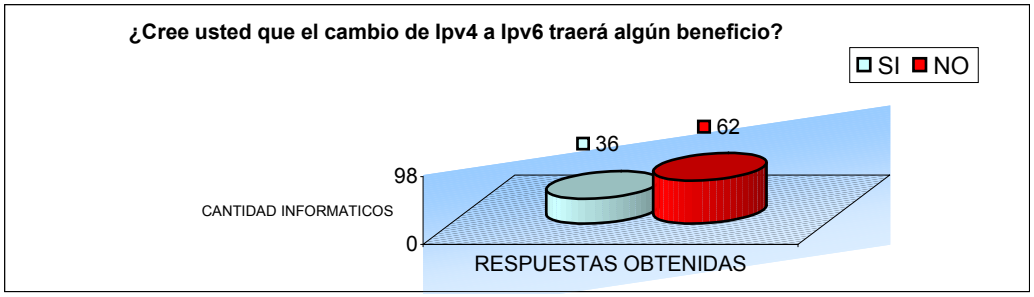
- Mayor rango de direcciones
- Mayor seguridad
- Escalabilidad
- Mejor desempeño

Sin embargo, existe una serie de características adicionales que si bien no son tan notorias; si van a tener mucho que ver con el comportamiento y configuración en las redes IPv6.

7 ¿Cree usted que el cambio de IPv4 a IPv6 traerá algún beneficio?

Esta pregunta se evaluó con dos opciones posibles sí y no; sin embargo, si el encuestado respondía que sí se le preguntaba por tres beneficios:

Gráfico 10



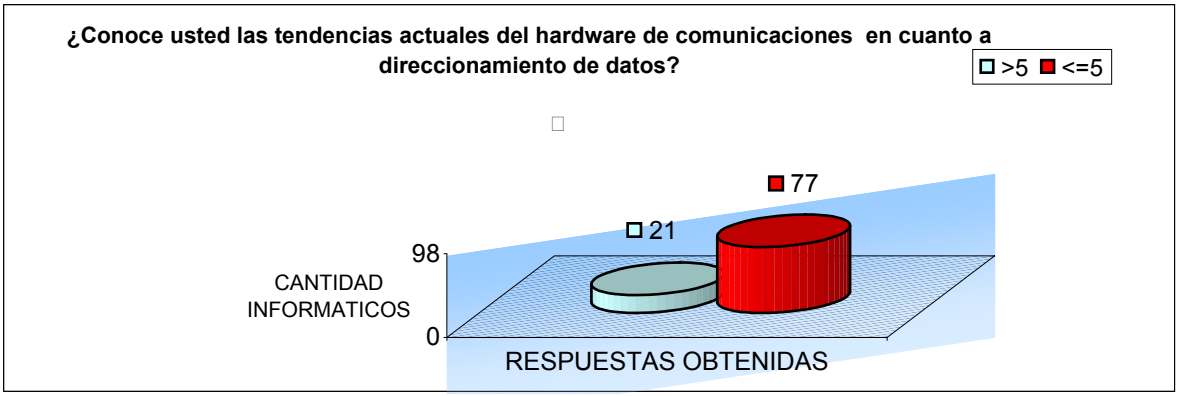
La respuesta tan negativa obtenida se debe quizás al desconocimiento del tema ya que con sólo compararlos se nota una gran serie de beneficios que se obtendrán con el nuevo protocolo; lo que reitera la necesidad de informar sobre este tema. Al consultar los beneficios que traerá consigo el nuevo protocolo a las personas que indicaron saberlos, todas fueron correctas lo que confirma su conocimiento; entre las respuestas obtenidas las más coincidentes fueron:

- Mayor capacidad
- Mayor seguridad
- Mayor eficiencia y eficacia en la administración

8 ¿Conoce usted las tendencias actuales del hardware de comunicaciones en cuanto a direccionamiento de datos?

Esta pregunta se evaluó con una escala del 1 a 10; el resultado obtenido es el siguiente:

Gráfico 11



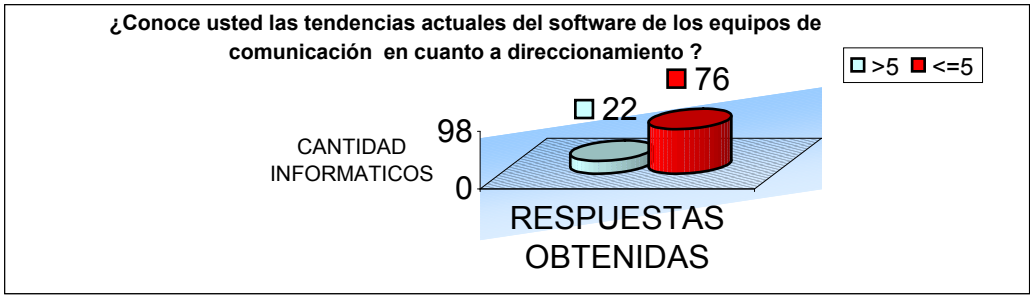
Fuente: Cuestionario aplicado a la población informática costarricense.

Existe gran desconocimiento en cuanto a hardware de comunicaciones y sus tendencias actuales en cuanto direccionamiento; esto va ligado con el desconocimiento de IPv6 y la plataforma física necesaria para darle soporte; es necesario ahondar en este subtema en la investigación como parte de la formación de un conocimiento sólido y completo sobre el tema en cuestión. Hasta que los profesionales comiencen a pensar en el cambio y conozcan por lo menos su idea básica; entonces empezarán a relacionar los productos que tiene el mercado y su compatibilidad y tendencias futuras; y comenzarán a notar cómo el mercado se dirige a la implementación de estructuras de comunicaciones soportadas por el protocolo de Internet versión 6.

¿Conoce usted las tendencias actuales del software de los equipos de comunicación en cuanto a direccionamiento ?

Esta pregunta se evaluó con una escala del 1 a 10; el resultado obtenido es el siguiente:

Gráfico 12



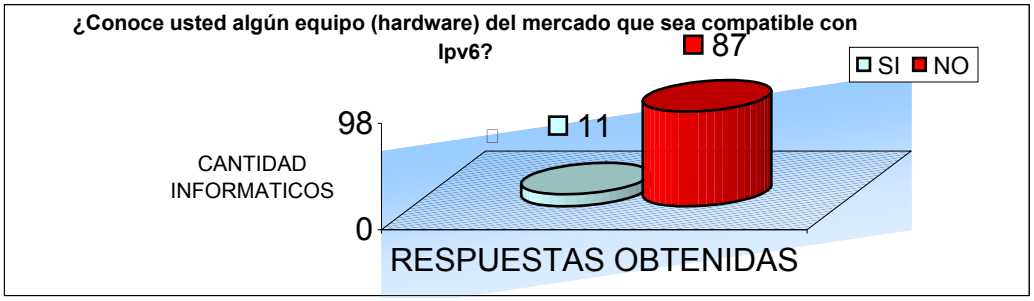
Fuente: Cuestionario aplicado a la población informática costarricense.

Al igual que en el hardware de comunicaciones, el software también es bastante desconocido y es necesario abarcar este sub-tema en la investigación. Al igual que el hardware hasta que los profesionales comiencen a investigar y empaparse el tema del cambio de protocolo, empezarán a descubrir el soporte adicional que poseen las grandes o principales aplicaciones comerciales y de mayor uso en cuanto a soporte para IPv6.

11 ¿Conoce usted algún equipo (hardware) del mercado que sea compatible con IPv6?

Esta pregunta se evaluó con dos opciones posibles sí y no; sin embargo, si el encuestado respondía que sí se le preguntaba por tres equipos conocidos.

Gráfico 13

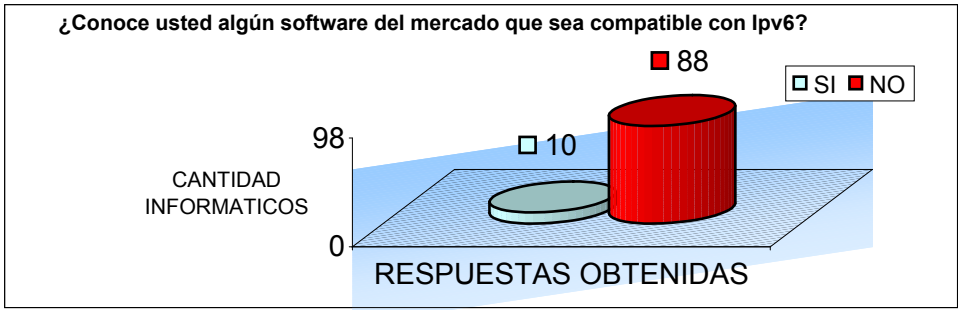


La respuesta obtenida confirma el desconocimiento en cuanto a la tendencia del hardware; por lo cual se debe tomar en cuenta en la investigación; se hablará en general de algunos equipos pero sin entrar en detalle ya que esto depende de la arquitectura de cada red. Entre los equipos más conocidos que soportan a IPv6 están los routers y los switches, según la opinión de los encuestados.

12 ¿Conoce usted algún software del mercado que sea compatible con IPv6?

Esta pregunta se evaluó con dos opciones posibles sí y no; sin embargo si el encuestado respondía que sí se le preguntaba por tres equipos conocidos.

Gráfico 14



Fuente: Cuestionario aplicado a la población informática costarricense.

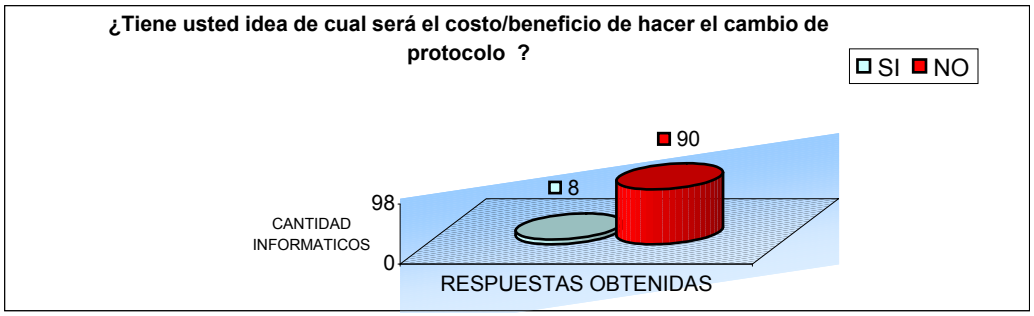
El conocimiento en cuanto a software es muy similar al del hardware por lo que también se debe informar sobre este tema ya que los dos van de la mano. De las 10

respuestas obtenidas, las más reiteradas fueron Windows (varias versiones), Linux y el sistema operativo de redes de cisco (Cisco IOS).

13 ¿Tiene usted idea de cuál será el costo/beneficio de hacer el cambio de protocolo ?

Esta pregunta se evaluó con dos opciones posibles sí y no.

Gráfico 15



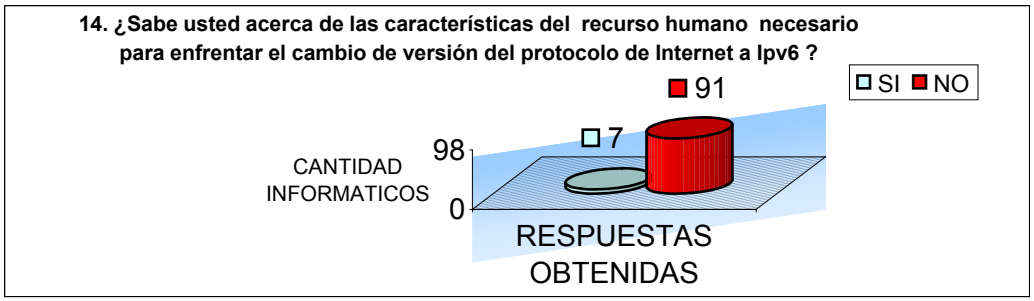
Fuente: Cuestionario aplicado a la población informática costarricense.

En las empresas, sea cual sea su actividad es necesario justificar los proyectos o las inversiones con una relación costo/beneficio; y este caso no se escapa de la regla; es importante justificar el cambio de protocolo como una inversión con un costo menor a sus múltiples beneficios para que esto llegue a ser una realidad en nuestra empresa y poder seguir siendo competitivos en un mundo donde las comunicaciones juegan papeles cada día más importantes.

14 ¿Sabe usted acerca de las características del recurso humano necesario para enfrentar el cambio de versión del protocolo de Internet a IPv6 ?

Esta pregunta se evaluó con dos opciones posibles sí y no; sin embargo si el encuestado respondía que sí se le preguntaba por algunas características.

Gráfico 16



Fuente: Cuestionario aplicado a la población informática costarricense.

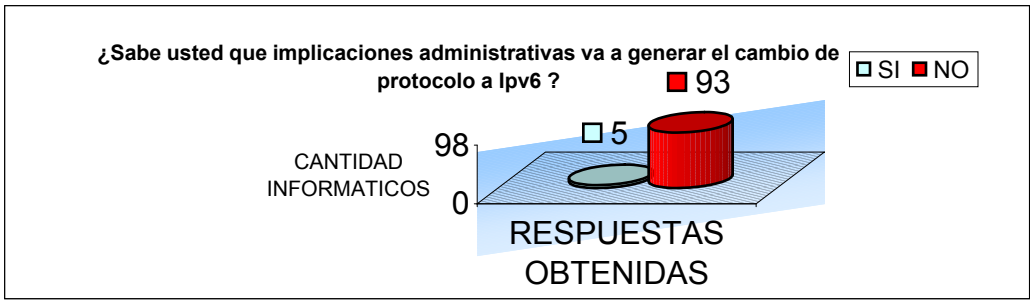
En todo proceso de cambio hay un factor muy importante que es el recurso humano; el cual al fin y al cabo es quien va a planear, ejecutar y controlar todo el proceso; por eso es importante incluirlo en la investigación formando por lo menos un perfil con las características requeridas para enfrentar el cambio; la parte de conocimientos necesarios es la que se trata de afirmar en este documento. En cuanto a las respuestas obtenidas al consultar cuáles eran algunas de las características, las más reiteradas fueron:

- Amplio conocimiento en redes
- Conocimientos de las versiones del protocolo de Internet 4 y 6.

15 ¿Sabe usted qué implicaciones administrativas va a generar el cambio de protocolo a IPv6 ?

Esta pregunta se evaluó con dos opciones posibles sí y no.

Gráfico 17



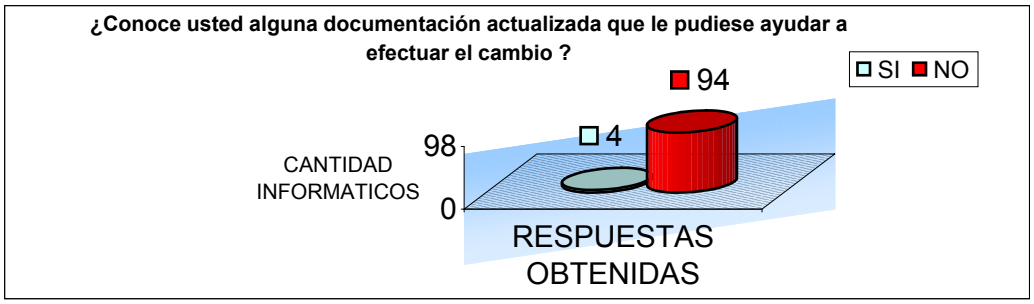
Fuente: Cuestionario aplicado a la población informática costarricense.

Al igual que el costo/beneficio se debe manejar qué implicaciones administrativas se podrían tener con un eventual cambio en la versión del protocolo. Esto para ampliar y mejorar el criterio de cambio ya que esto ayudará a justificarlo de mejor manera al conocer como afecta la parte administrativa de la empresa que al final es la que va a ayudar a que la transición de protocolos sea todo un éxito al facilitar los recursos necesarios.

16 ¿Conoce usted alguna documentación actualizada que le pudiese ayudar a efectuar el cambio ?

Esta pregunta se evaluó con dos opciones posibles sí y no; sin embargo, si el encuestado respondía que sí se le preguntaba por los documentos.

Gráfico 18

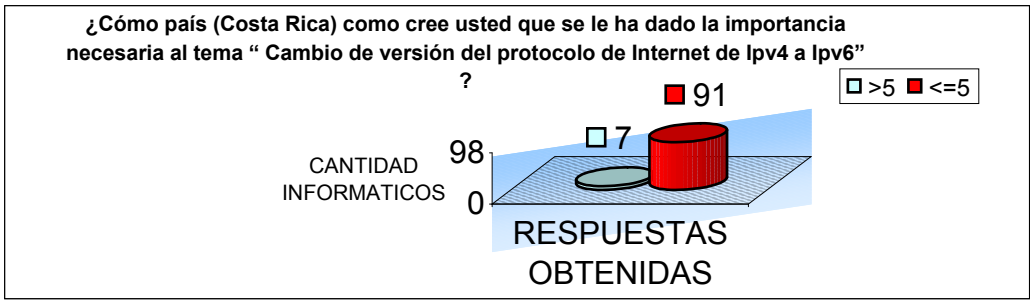


Los resultados demuestran la escasez de documentación o información en el medio sobre este tema. Uno de los objetivos principales de esta investigación es producir una documentación básica actualizada y acorde a las necesidades de la comunidad informática costarricense que sirva de base principal para luego enfrentar cada caso en particular representado por la infraestructura de cada empresa. Al pedir que se refirieran a la documentación conocida, 4 de 6 personas concuerdan en documentos o artículos de Internet; lo cual hace un poco informal la fuente.

17 ¿Cómo país (Costa Rica) cree usted que se le ha dado la importancia necesaria al tema " Cambio de versión del protocolo de Internet de IPv4 a IPv6"?

Esta pregunta se evaluó con una escala del 1 a 10; el resultado obtenido es el siguiente:

Gráfico 19



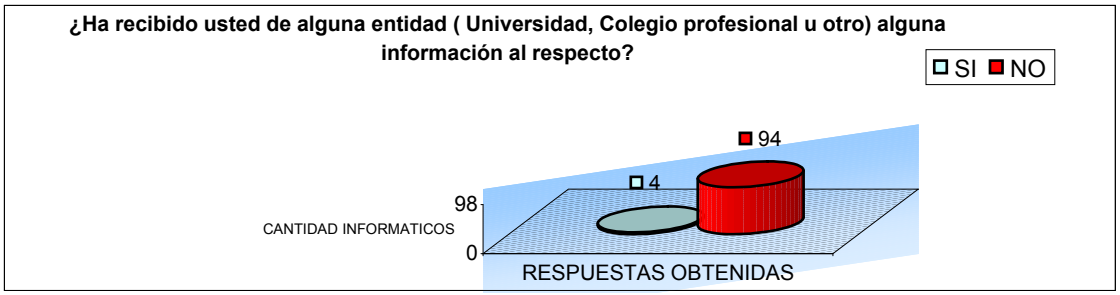
Fuente: Cuestionario aplicado a la población informática costarricense.

El resultado refleja la poca importancia que se le ha dado al tema como país en conjunto; lo cual debería de ser muy tomado en cuenta por entes públicos o privados que intervengan el desarrollo tecnológico del país y reforzar este tema con la publicación y/o distribución de documentos. En este caso al terminar y ser revisado y aprobado el documento se tratará de difundir por medio del Colegio Profesional y el Ministerio de Ciencia y Tecnología.

18 ¿Ha recibido usted de alguna entidad (Universidad, Colegio profesional u otro) alguna información al respecto?

Esta pregunta se evaluó con dos opciones posibles sí y no; sin embargo, si el encuestado respondía que sí, se le preguntaba por la fuente de información.

Gráfico 20



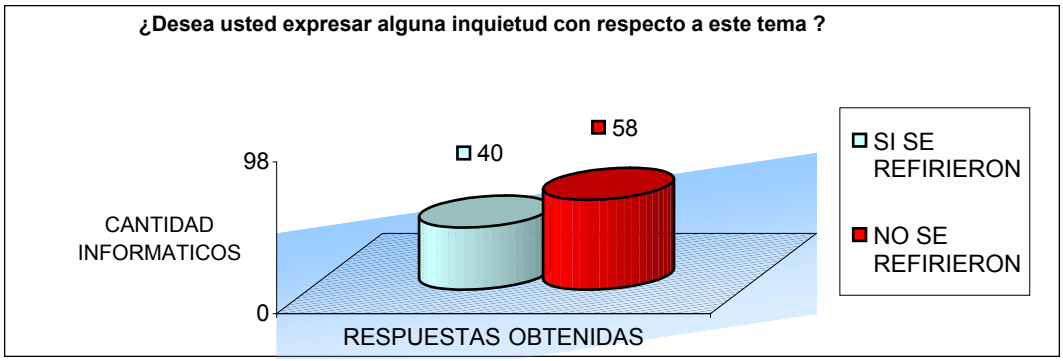
Fuente: Cuestionario aplicado a la población informática costarricense.

Se evidencia un desconocimiento de este tema; lo cual se tratará de mejorar con la elaboración y divulgación del presente documento. Al consultar cuál fue la fuente de la información de las 4 respuestas obtenidas todas coincidieron en que la habían recibido en la universidad. Sin embargo, se ha tratado como un tema aislado y de menor relevancia, lo que se refuta con solo tratar de informarse un poco sobre el tema.

19 ¿Desea usted expresar alguna inquietud con respecto a este tema?

En esta pregunta se dieron algunas líneas para que se expresaran en cuanto al tema. El resultado fue el siguiente:

Gráfico 21



Fuente: Cuestionario aplicado a la población informática costarricense.

Del total de la muestra sólo el 40% quiso expresar sus inquietudes; de las cuales se destacan:

- El deseo de obtener información sobre el tema.
- Después de esta entrevista, algunos iban a investigar un poco más sobre el tema.
- Se solicita mayor información y divulgación sobre el tema.
- Algunos simplemente dijeron que no conocían bien el tema.

5. Conclusiones y Recomendaciones

Conclusión

Los informáticos costarricenses tienen un nivel de conocimiento aceptable con respecto al protocolo de Internet; sin embargo, existe una pequeña porción de la población que no lo tiene.

Recomendación

Con el fin de cubrir toda la población informática costarricense se debe difundir información sobre el tema; esta función le corresponde al Ministerio de Ciencia y Tecnología y debe de hacerlo mediante charlas, conferencias, foros y boletines.

En este documento se debe presentar una introducción al tema del protocolo de Internet que contemple aspectos generales para lograr estandarizar el nivel de conocimiento; y así tener una base aceptable.

Conclusión

El conocimiento que se tiene de la nueva versión del protocolo de Internet (IPv6) es muy escaso.

Recomendación

También por su campo de acción, el divulgar información sobre el IPv6 compete al Ministerio de Ciencia y Tecnología, quien debe promover la información entre la población mediante charlas, conferencias, foros y boletines.

Se debe plasmar en este documento información general acerca de "IPv6".

Conclusión

No se tiene conciencia del beneficio que puede acarrear el cambio de protocolo.

Recomendación

Se debe informar y concientizar al informático costarricense con respecto a los beneficios que acarrea el cambio de protocolo. Esta parte le corresponde al Colegio de

Profesionales en Informática y Computación (CPIC); quien debe buscar los medios para difundir información al respecto entre sus agremiados y mostrar el impacto que este nuevo protocolo puede tener en las organizaciones.

Conclusión

Es poco el conocimiento que se tiene acerca de la tendencia del hardware y software de comunicaciones en cuanto a direccionamiento de datos.

Recomendación

Se debe informar acerca de las tendencias actuales del hardware y software de comunicaciones y direccionamiento, mediante la ejemplificación de las acciones y contribuciones hechas por los principales fabricantes del mercado de las comunicaciones.

Conclusión

Se desconocen los equipos y software del mercado compatibles con "IPv6".

Recomendación

Se debe mostrar cómo los principales fabricantes de equipos y software del mercado ya han incorporado características compatibles con "IPv6" en sus productos.

Conclusión

Se desconoce el costo/beneficio que podría traer un cambio de versiones.

Recomendación

Se debe mostrar la relación costo/beneficio que acarrea el cambio hacia el "IPv6". Esto mediante ejemplos y estudios realizados por organizaciones a nivel mundial que actualmente están tomando la iniciativa; colaborando y comprometiéndose con el cambio hacia la nueva generación del protocolo de Internet.

Conclusión

Se desconoce acerca del nivel de conocimiento que debe tener el recurso humano para enfrentar el cambio de protocolos.

Recomendación

Se debe especificar una serie de características que debe tener el recurso humano para enfrentar el cambio de versiones, con el fin de ayudar a preparar el cambio en su organización.

Conclusión

Se desconocen las implicaciones administrativas que va a generar el cambio de versiones del protocolo de Internet.

Recomendación

Se debe informar sobre las implicaciones administrativas que podría generar el cambio de versiones, tomando en cuenta una serie de características generales que podrían tener en común las empresas.

Conclusión

Se desconocen los documentos formales acerca del tema de cambio de versiones del protocolo de Internet.

Recomendación

Se debe informar y facilitar a la comunidad informática sobre otros documentos, boletines, sitios web, foros, que puedan ayudarle a obtener la información requerida para poder enfrentar el cambio.

Conclusión

En Costa Rica es poca la importancia que se le ha dado al tema del cambio de versiones del protocolo de Internet.

Recomendación

Se debe comentar, tratar y difundir entre los miembros de la comunidad informática costarricense documentos acerca el tema, para así crear conciencia de su importancia. Esto compete en primera instancia al Ministerio de Ciencia y Tecnología, al Colegio Profesional, las Universidades públicas y privadas y a toda aquella organización que apoye el fortalecimiento tecnológico del país.

6. Desarrollo de la propuesta

6.1 Introducción

Para comunicar las redes u ordenadores se desarrollaron varios protocolos; entre ellos el protocolo de Internet "IP" y los protocolos de control de transmisión "TCP". Debido a que el Protocolo Internet está específicamente limitado a proporcionar las funciones necesarias para enviar un paquete de bits (un datagrama Internet) desde un origen a un destino a través de un sistema de redes interconectadas y TCP es un protocolo confiable, orientado a conexión; suministra control de flujo y confiabilidad a través de los números de secuencia y acuses de recibo. De esta manera TCP vuelve a enviar cualquier mensaje que no se reciba. La ventaja de TCP es que proporciona una entrega garantizada de los segmentos.
Posteriormente estos protocolos se combinaron formando así el conjunto de protocolos TCP/IP.

El conjunto de Protocolo de Control de Transmisión / Protocolo Internet (TCP/IP) originalmente se desarrolló para suministrar comunicaciones a través de DARPA. Posteriormente se incluyó en la Distribución del Software Berkeley de UNIX lo que ayudó a su expansión por todo el mundo, ya que este sistema operativo se distribuía libremente por las Universidades. TCP/IP es hoy el estándar mundial para las comunicaciones entre redes y sirve como el protocolo de transporte para Internet, logrando que millones de computadores se comuniquen a nivel mundial. TCP/IP permite la comunicación entre cualquier conjunto de redes interconectadas y sirve tanto para las comunicaciones de LAN como de WAN.

Finalmente en 1983 nació Internet, que también utiliza este protocolo para la interconexión de redes debido a sus grandes ventajas como la independencia del fabricante, su capacidad de soportar múltiples tecnologías y su capacidad de funcionar en máquinas de cualquier tamaño.

Cuando la versión actual de este protocolo se desarrolló, no se tuvieron en cuenta todas las posibilidades reales que este nuevo medio de comunicación podía

ofrecer. Por otra parte, muchas de ellas eran inimaginables en aquellos días, por lo que resulta lógico que sucediera. Actualmente, es tal el desarrollo de Internet en el mundo, que la antigua versión de IP (versión 4) se está quedando pequeña y para determinadas actividades y servicios resulta bastante pobre, por lo que se estaba haciendo necesario una revisión de este protocolo para no limitar las enormes posibilidades que la conexión global del planeta puede ofrecer. Por este motivo, se pensó hacer una nueva versión para adaptarse a los tiempos modernos. Es cuestión de "renovarse o morir" y una vez que se vieron todas las posibilidades que ofrecía Internet, resultaba muy duro tener que morir.

El motivo principal por el que surge en el seno del IETF ("Internet Engineering Task Force") la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng ("Internet Protocol Next Generation" o Siguiente Generación del Protocolo Internet), fue la evidencia de la falta de direcciones.

IPv4 tiene un espacio de direcciones de 32 bits, es decir 2^{32} (4.294.967.296).

En cambio, IPv6 ofrece un espacio de 2^{128}
(340.282.366.920.938.463.463.374.607.431.768.211.456).

A manera de ejemplo y para hacerse a la idea de lo que esta cifra "impronunciable" implica se puede calcular el número de direcciones IP que se podría tener por metro cuadrado de la superficie terrestre; nada más y nada menos que 665.570.793.348.866.943.898.599.

Indudablemente, hay cabida para todos los dispositivos que se puedan imaginar, no sólo terrestres, sino interplanetarios. Aunque, por el momento no se puede asegurar que tenga capacidad para los dispositivos "intergalácticos".

Desde hace mucho tiempo, debido al crecimiento y a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico.

Entre los "parches" más conocidos, se pueden citar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec), y Movilidad, fundamentalmente.

El inconveniente más importante de estas ampliaciones de IPv4 es que utilizar cualquiera de ellos es muy fácil, pero no tanto cuando se pretende usar al mismo tiempo dos o tres, pues llega a ser un auténtico malabarismo de circo. Además, IPv4 tiene otros problemas o "dificultades" que IPv6 soluciona o mejora.

6.2 ¿Por qué IPv6?

Como anteriormente se citó la ventaja fundamental de IPv6 es el espacio de direcciones.

El reducido espacio de IPv4, a pesar de disponer de cuatro mil millones de direcciones (4.294.967.296), junto al hecho de una importante falta de coordinación durante la década de los 80 en la asignación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos, está llevando a límites no sospechados en aquel momento.

Por supuesto, hay una solución que se podría considerar como evidente, como sería la renumeración, y reasignación del espacio de direcciones.

Sin embargo, no es tan sencillo. Es incluso impensable en algunas redes, ya que requiere unos esfuerzos de coordinación, a escala mundial, absolutamente impensables.

Además, uno de los problemas de IPv4 permanecería: la gran dimensión de las tablas de enrutamiento en Internet, que la hace ineficaz y perjudica enormemente los tiempos de respuesta.

La falta de direcciones no es apreciable por igual en todos los puntos de la red, de hecho, no es casi apreciable por el momento en Norte América. Sin embargo, en zonas geográficas como Asia (en Japón la situación esta llegando a ser crítica), y Europa, el problema se agrava.

Como ejemplos, se puede citar el caso de China que ha pedido direcciones para conectar 60.000 escuelas, tan sólo ha obtenido una clase B (65.535 direcciones), o el

de muchos países Europeos, Asiáticos y Africanos, que sólo tienen una clase C (255 direcciones) para todo el país.

Tanto en Japón como en Europa el problema es creciente, dado el importante desarrollo de las redes de telefonía celular, inalámbricas, módems de cable, xDSL("digital subscriber line" línea de suscriptor digital), que requieren direcciones IP fijas para aprovechar al máximo sus posibilidades e incrementar el número de aplicaciones en las que pueden ser empleados.

La razón de utilización de las direcciones IP por parte de los usuarios y está pasando en pocos meses de 10:1(una dirección para 10 usuarios) a 1:1, y la tendencia se invertirá. En pocos meses, se podrá ver dispositivos "siempre conectados", con lo que fácilmente un usuario podría tener, en un futuro no muy lejano, hasta 50 o 100 IP's (1:50 o 1:100).

Algunos Proveedores de Servicios de Internet se ven incluso obligados a proporcionar a sus clientes direcciones IP privadas, mediante mecanismos de NAT (traslación de direcciones, es decir, usar una sola IP pública para toda una red privada). De hecho, casi todos los PSI's (ISP; proveedores de servicios de Internet) se ven obligados a delegar tan sólo reducidos números de direcciones IP públicas para sus grandes clientes corporativos.

Como ya se ha dicho, la solución, temporalmente, es el uso de mecanismos NAT.

Desafortunadamente, de seguir con IPv4, esta tendencia no sería "temporal", sino "invariablemente permanente". Ello implica la imposibilidad práctica de muchas aplicaciones, que quedan relegadas a su uso en Intranets, dado que muchos protocolos que son incapaces de atravesar los dispositivos NAT: RTP y RTCP ("Real-time Transport Protocol" y "Real Time Control Protocol") usan UDP con asignación dinámica de puertos (NAT no soporta esta traslación).

La autenticación Kerberos necesita 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 tan complicada con NAT que en la práctica no se emplea.

6.3 Cifras actuales y proyecciones del crecimiento de Internet

Las cifras de "internautas", esperadas en los próximos años, avalan lo expuesto:

- África: 800.000.000 (sólo 3.000.000 sin NAT)
- América Central y del Sur: 500.000.000 (sólo 10.000.000 sin NAT)
- América del Norte: 500.000.000 (sólo 125.000.000 sin NAT)
- Asia: 2.500.000.000 (sólo 50.000.000 sin NAT)
- Europa Occidental: 250.000.000 (sólo 50.000.000 sin NAT)

Pero lo más importante es el imparable crecimiento de aplicaciones que necesitan direcciones IP públicas únicas, globales, válidas para conexiones extremo a extremo, y por tanto encaminables (enrutables): Videoconferencia, Voz sobre IP, seguridad, e incluso juegos.

Veamos más cifras. Sólo en Estados Unidos de América, el mercado potencial de aplicaciones susceptibles de ser conectadas a la red, según " Driscol & Associates", en un estudio de 1.995 se ve en el siguiente cuadro:

MERCADO VERTICAL	EJEMPLOS DE APLICACIÓN	TAMAÑO DEL MERCADO
Lectura de Contadores	Lectura de consumos de agua, gas, electricidad, etc.	242.000.000
Seguridad	Sistemas de alarma, incendios, etc., tanto residenciales como comerciales	24.000.000
Posicionamiento de Vehículos/flotas e información de condiciones	Seguimiento automático de vehículos Seguimiento de inventarios Diagnóstico y seguridad de vehículos	15.000.000
Monitorización	Máquinas de venta automática (vending) Buzones de correo Gas e irrigación	7.900.000
	Total	**288.900.000**

Fuente: Driscol & Associates.

En 1.997 el mercado de dispositivos con aplicaciones capaces de conectarse a Internet (sin incluir terminales ni ordenadores, tan sólo WebTV, agendas electrónicas, teléfonos con acceso a Internet y consolas de juegos) era de 3.000.000. En 1.998, este se duplica hasta llegar a los 6.000.000. Sólo contabilizando el crecimiento de la nueva generación de telefonía móvil (UMTS), en el 2.003 se sobrepasaron las cifras del orden de los 1.000.000.000 de usuarios, la misma cifra que para la telefonía fija y que para el

número de usuarios "fijos" de Internet. En ese momento, los usuarios móviles con conexión a Internet superan a los 400.000.000.

El Foro UMTS/GSM prevé unas necesidades de direcciones IP para los dispositivos de la red (no para los dispositivos de los usuarios), para el 2.005 de 3,2 millones, y de 6,3 para el 2.010. Según ellos, en el 2.005, se requerirían un total de 20.000.000.000 de direcciones IP para los dispositivos de los usuarios.

A esto se ha de sumar los innumerables dispositivos que se van creando, o los ya existentes a los que se dan nuevas o mejoradas aplicaciones, mediante su conexión a la red. Por ejemplo:

- Teléfonos, pues la siguiente generación, sin duda, pasará por tecnologías IP (VoIP).
- Televisión y Radio, también basados en tecnologías IP.
- Sistemas de seguridad, televigilancia y control.
- Frigoríficos que evalúan nuestros hábitos de consumo y nos dan la opción de
- imprimir la lista de la compra,
- Hacer el pedido en el supermercado para que nos sea entregado automáticamente,
- Hacer el pedido para que pasemos a recogerlo, decidiendo "in situ" el resto de la compra,
- Navegar por un supermercado virtual y permitirnos llenar el carro según nuestros hábitos, añadiendo nuestros caprichos ocasionales.
- Despertadores que conocen nuestros tiempos de desplazamiento habituales a nuestro lugar de trabajo, y con motivo de un accidente o gran nevada, de los que son informados mediante los servicios de la red, calculan el tiempo adicional que necesitamos y nos levantan con la anticipación precisa, ¡aún a riesgo de que los destrocemos al arrojarlos contra la pared!
- Walkman MP3, que conectados a la red permiten recuperar y almacenar creaciones musicales.
- Nuevas tecnología emergentes, como Bluetooth, redes inalámbricas, redes domésticas, hacen más patente esta necesidad de crecimiento, al menos, en lo que al número de direcciones se refiere. Por ejemplo, la última tendencia es la

de permitir a cualquier dispositivo serie ser conectado a una LAN o WAN, y por qué no a Internet. Este tipo de "convertidores", denominados "Universal Device Server", o Servidor de Dispositivos Universal, permite que aplicaciones impensables por las limitaciones de los cableados en serie, se realicen remotamente a través de redes, o incluso que un sistema de alarmas, que antes requería un módem dedicado para la conexión con la central de recepción de alarmas, pueda ahora enviar un e-mail, ¡con todo lujo de detalles!.

Se podría hablar, en general, de casi cualquier dispositivo tanto doméstico como industrial, integrado en la gran red, pero también en dispositivos de control médico, por ejemplo el marcapasos.

6.4 Características principales de IPv6

En resumen, las características principales de IPv6 son las siguientes:

- Mayor espacio de direcciones.
- "Plug & Play": autoconfiguración.
- Seguridad intrínseca en el núcleo del protocolo (IPsec).
- Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: Envío de UN mismo paquete a un grupo de receptores.
- Anycast: Envío de UN paquete a UN receptor dentro de UN grupo.
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los enrutadores (routers), alineados a 64 bits (preparados para su procesado óptimo con los nuevos procesadores de 64 bits), y con una cabecera de longitud fija más simple que agiliza su procesado por parte del enrutador (router).
- Posibilidad de paquetes con carga útil (datos) de más de 65.535 bytes.
- Enrutado más eficiente en el troncal (backbone) de la red, debido a una jerarquía de direccionamiento basada en la agregación.
- Renumeración y "multi-homing", que facilita el cambio de proveedor de servicios.
- Características de movilidad.

Además de que estas son las características básicas, la propia estructura del protocolo permite que este crezca con ”escalabilidad”, según las nuevas necesidades y aplicaciones o servicios lo vayan precisando. Precisamente, la escalabilidad es la ventaja más importante de IPv6 frente a IPv4.

6.5 Reservas de espacio de direccionamiento en IPv6

A diferencia de las asignaciones de espacio de direccionamiento que se hicieron en IPv4; en IPv6 se ha reservado sin asignar algo más del 15% del total de direcciones especiales, tanto para permitir una fácil transición, como para mecanismos requeridos por el propio protocolo.

El tipo específico de una dirección IPv6 queda determinado por los primeros bits. La asignación actual de los prefijos se muestra en la siguiente tabla.

Tabla N° 2

Estado	Prefijo (en binario)	Fracción del Espacio
Reservado	0000 0000	1/256
No Asignado	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 010	1/128
No Asignado	0000 011	1/128
No Asignado	0000 1	1/32
No Asignado	0001	1/16
Direcciones Unicast Globales Agregables	001	1/8
No Asignado	010	1/8
No Asignado	011	1/8
No Asignado	100	1/8
No Asignado	101	1/8
No Asignado	110	1/8
No Asignado	1110	1/16
No Asignado	1111 0	1/32
No Asignado	1111 10	1/64
No Asignado	1111 110	1/128
No Asignado	1111 1110 0	1/512
Direcciones Unicast Locales de Enlace	1111 1110 10	1/1.024
Direcciones Unicast Locales de Sitio	1111 1110 11	1/1.024
Direcciones Multicast	1111 1111	1/256

Fuente: Ipv6 Forum

De esta forma se permite la asignación directa de direcciones de agregación, direcciones locales y multicast, con reservas para OSI NSAP e IPX. El 85% restante queda reservado para necesidades y uso futuros.

6.6 Mecanismos de Transición "IPv4"/"IPv6"

Coexistencia con "IPv4" y migración

En un principio para la implantación del "IPv6" se deberá utilizar mecanismos de transición debido a las siguientes razones:

Con el protocolo de Internet "IPv6" no existe una fecha o lapso para la implantación; en un principio, la mayor parte de las redes estarán trabajando en "IPv4".

"IPv4" e "IPv6" son incompatibles a nivel de paquete.

Los routers actuales "IPv4" descartan los paquetes "IPv6".

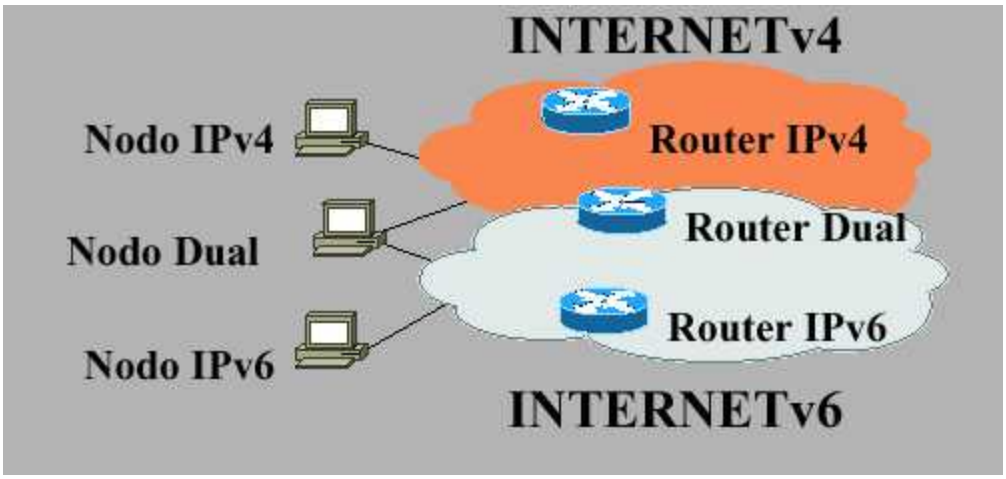
Existe un incontable número de host y routers que manejan "IPv4". Sería casi impensable el reemplazar todos estos equipos de una sola vez.

El diseño de "IPv6" permitirá la coexistencia con "IPv4" por un tiempo; el cual parece que va a ser muy largo.

Por lo tanto, la estrategia principal de migración consiste en proveer la interconexión de nodos "IPv6" a través de las redes actuales de "IPv4".
Para ello existen mecanismos que pueden ser implementados tanto a nivel de host como de router; los cuales facilitan la transición. Quizás de allí se desprende un hecho clave de "IPv6" que es la compatibilidad con "IPv4", que permitirá una transición en forma escalonada y controlada, lo cual sin duda llevará a un proceso de transición exitoso.

Según en el punto será necesario seguir una de las siguientes estrategias: Si la implantación es a nivel de host/router, la solución es conocida como "dual Stack"; si la solución es a nivel de red entonces se requiere la tunelización; si es a nivel de gateway lo que se requiere son los traductores "IPv6"/"IPv4".

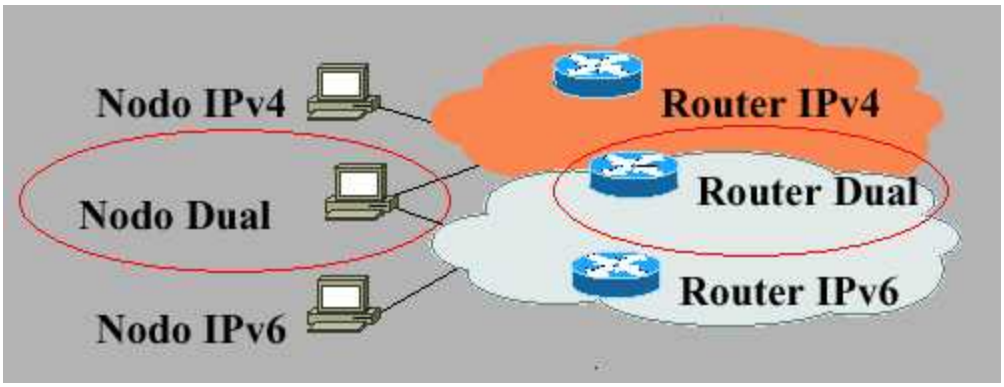
Durante la etapa de implantación se verá a nivel lógico que existirán dos clases de Internet: Internet v4 e Internet v6; ambas versiones interactúan mediante la implantación de nodos duales; los cuales sirven de puente entre nodos "IPv4" e "IPv6"; debido a su capacidad de trabajar ambos protocolos.



Para el logro de este objetivo se recomienda la utilización de las técnicas que a continuación se detallan:

En el host o router "Dual stack"

La forma más simple para que los nodos o routers tengan compatibilidad con "IPv4" es proveerlos de una configuración "IPv4" completa; lo cual permite los nodos "IPv6"; de esta manera los nodos que tengan estas características podrán enviar y recibir directamente paquetes "IPv4" e "IPv6"; por lo que son llamados "nodos "IPv4"/"IPv6" "



Para los nodos duales se deben utilizar direcciones de formato mixto, el cual consiste en representar la dirección de la siguiente manera X: X: X: X: X: X:D. D. D. D.; en donde las X representan los primeros conjuntos de 16 bits en exadecimal y las D; los 4 grupos restantes que componen los 32 bits de la dirección en formato decimal.

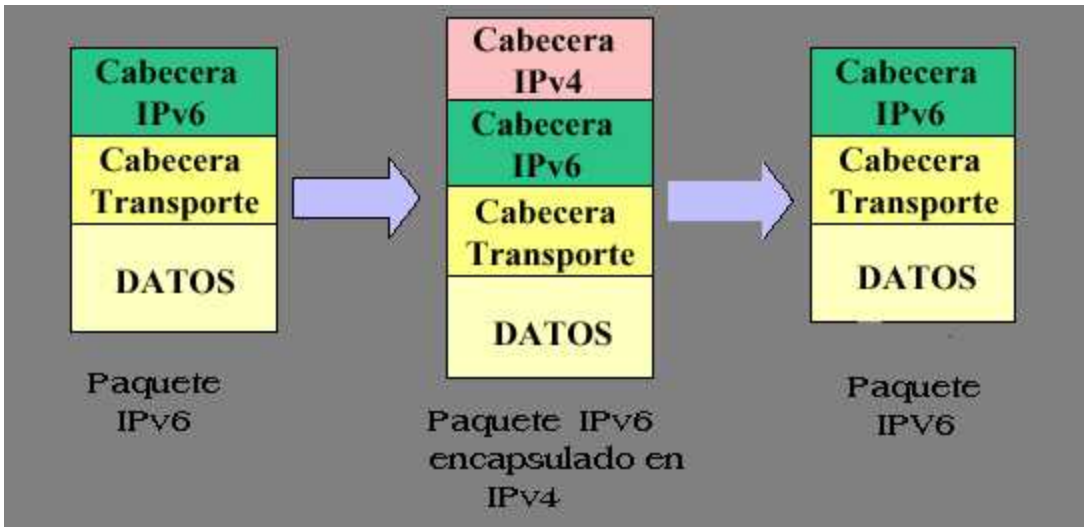
Ejemplo:

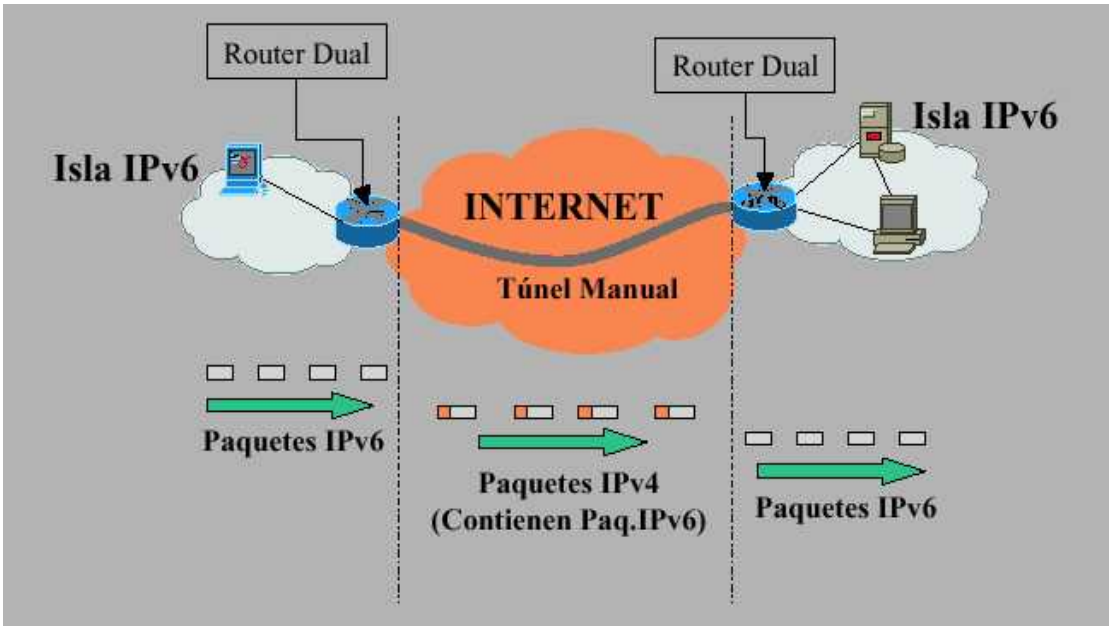
0: 0: 0: 0: 0: 0:192.168.240.14 en formato comprimido sería: 192.168.240.14

Nota: Recuerde que para "IPv4" se utilizarán sólo los últimos 32 bits y para "IPv6" se utilizarían los 132 bits o en su defecto la forma de representación comprimida.

En la red “Túneles configurados”

Como se ha indicado, en una metodología de implantación escalonada la infraestructura "IPv4" debe seguir funcionando y la manera de hacerlo es pasar paquetes "IPv6" encapsulados dentro de paquetes "IPv4".
El motivo principal de estos túneles es conectar dominios "IPv6" aislados en un entorno "IPv4”.





En este tipo de túnel los dos nodos son del tipo dual; debido a que en ambos se configura las direcciones "IPv6" e "IPv4"; tanto locales como remotas.

Una de las aplicaciones principales de este método es la conexión con los ISP "Proveedores de Servicios de Internet"

Entre sus inconvenientes están que no son dinámicos sino que los túneles se establecen manualmente mediante la asignación de direcciones y se usa para

interconectar N islas "IPv6" en un entorno "IPv4", entonces debe crearse igual número de túneles.

Cuando el paquete que se envía al router más cercano y este lo desencapsula a "IPv6" y lo reenvía basado en la dirección "IPv6" que el paquete provee; a esto se le llama túnel configurado o manual; ya que se están dando todas las direcciones requeridas para transportar el paquete hasta su destino final.

Si este no es el caso y el paquete se pasa a un router "IPv4" y este debe buscar la dirección del siguiente salto en su tabla de direcciones hasta llegar a un dispositivo "IPv4"/"IPv6" que desencapsule paquete y obtenga la dirección "IPv6" destino; a esto se llama túnel automático.

A estos túneles se les llama distinto según su función:

Túneles 6to4

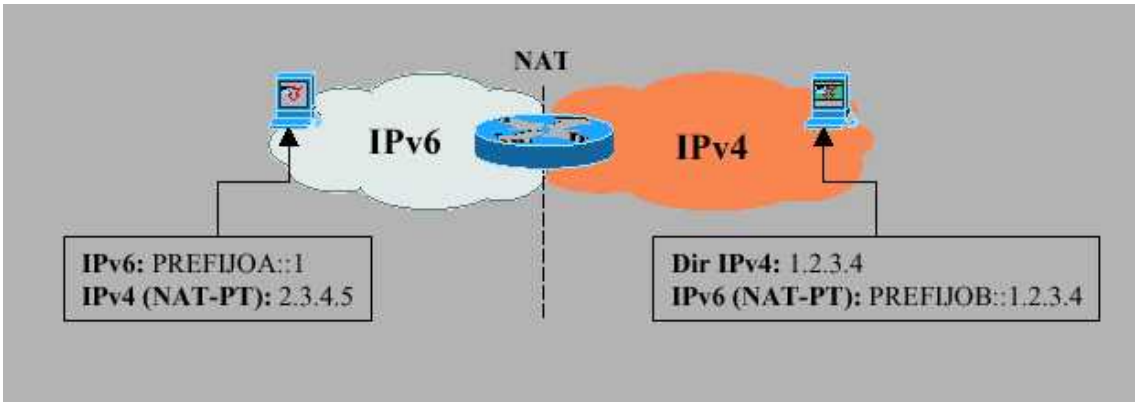
Su función es comunicar islas "IPv6" en un océano "IPv4"; en este caso las direcciones son convertidas de su dirección "IPv6" a una equivalente y notación "IPv4".

Túneles 6over4

Su función es comunicar islas "IPv6" dispersas en subredes "IPv4"; de manera que se forma una "LAN Virtual"; en la que el tráfico "IPv6" es encapsulado en paquetes IPv4 Multicast; lo que permite enviar el paquete a un grupo de direcciones a la vez.

En el gateway

El NAT (Traducción de Direcciones de Red) consiste en traducir direcciones en formato "IPv6" a "IPv4" y viceversa; según se requiera. Funciona manteniendo una tabla de mapeado de direcciones "IPv4" a direcciones "IPv6". Es un host fronterizo que funciona como gateway entre la red origen y la destino.



Una de las ventajas de la traducción NAT es que muchas empresas ya tienen conocimiento sobre esta metodología. Sin embargo, requiere un alto costo de gestión y administración.

El proceso de traducción de una dirección es más costoso (tiempo, administración) que el de túneles; y además requiere el uso de código especial o configuraciones adicionales si se necesita retransmitir algunos protocolos no amigables con NAT como el uso de "IPsec" (Protocolo de Seguridad IP).

6.7 Situación mundial de IPv6

Según el "Foro ipv6" se pueden identificar cinco regiones diferenciadas en lo que al estado de desarrollo de IPv6 se refiere:

a) Asia: en esta área el impacto de la falta de direcciones IPv4 ha sido más obvio, y APNIC, la entidad de registro regional de Internet para esta área (http://www.apnic.net) espera agotar su rango de direcciones IPv4 en muy pocos meses. En correspondencia, la presión para encontrar soluciones adecuadas es muy alta, y se han iniciado gran número de actividades, particularmente en Japón: WIDE(http://www.v6.wide.ad.jp),KAME (http://www.kame.net) y TAHI (http://www.tahi.org).
b) Europa: la industria de la telefonía móvil es un soporte muy fuerte para la transición a IPv6. En correspondencia, ETSI (European Telecommunications

Standards Institute) y el Foro IPv6 han establecido un acuerdo de cooperación para aunar sus fuerzas; este movimiento de ETSI ha sido tildado como impulsado por "el fuerte deseo de los operadores inalámbricos". Además de este acuerdo de cooperación con ETSI, el Foro IPv6 ha estrechado fuertes lazos con el Foro UMTS y la Asociación GSM, y hay conversaciones con el grupo 3GPP.

c) Norteamérica: muchas actividades relacionadas con IPv6, tanto en términos de estandarización y despliegue/verificación, tienen sus orígenes en esta región. Muchas de estas actividades pueden ser localizadas en torno al "6bone", la "plataforma de pruebas" internacional de IPv6 (http://6bone.net). Otras actividades relacionadas con IPv6 que incluyen importante participación norteamericana son 6REN (http://www.6ren.net) – iniciativa de coordinación para IPv6 en redes de investigación y educación, 6TAP (http://6tap.net) – iniciativa para proporcionar un router IPv6 central en Chicago para facilitar la interconexión entre redes IPv6, y Freenet/Viagénie (http://www.freenet6.net y http://www.viagenie.qc.ca) – iniciativa de túneles automáticos. En cualquier caso, el despliegue comercial de IPv6 en esta región se ha iniciado muy despacio; sólo hay 2 rangos de direcciones IPv6 comerciales (de un total de 22 en todo el mundo) en Norteamérica. Esto refleja la apariencia de que el despliegue operacional de IPv6 "puede no llegar primero a ésta área" (tal y como ha sido indicado en el encuentro 46º del IETF, grupo de trabajo IPng), ya que los problemas de la falta de direcciones IPv4 aún no han emergido como una urgencia en esta región.

d) Rusia: las fuertes relaciones entre el Foro IPv6, el Foro IPv6 local Ruso, y FREEnet (red académica y de investigación Rusa) tienen como objetivo crear una comunidad rusa de usuarios de IPv6 y proveedores de servicios y soluciones.

e) Resto del Mundo: a corto plazo, veremos muchos ejemplos de nuevas actuaciones en México, Corea, India, Australia y Singapur. No es tan extraño dado que son países con alto nivel tecnológico (India) o están situados entre dos grandes áreas de desarrollo (Australia, entre Japón y US). En Singapur la razón es el alto grado de comunicaciones inalámbricas, por medios muy diversos.

En Costa Rica no se ha dado la importancia requerida a este tema; como se ha hecho en otros países como España en donde se formó el "IPv6 Task force " con el fin de definir una estrategia de la industria española para afrontar el cambio. Como parte de esta iniciativa se convocó al Ministerio de Ciencia y Tecnología español y se dieron entre otras recomendaciones las siguientes:

1. Incrementar la presencia de la industria y la comunidad académica española en proyectos nacionales, europeos e internacionales relacionados con "IPv6".
2. Favorecer la difusión y formación en "IPv6" en la comunidad empresarial española.
3. Incrementar las actividades de investigación aplicadas en la industria y en la comunidad académica española.
4. Aumentar la presencia española en las labores de estandarización de "IPv6".
5. Apoyar e impulsar las iniciativas del sector privado para el desarrollo de nuevas redes, servicios y aplicaciones "IPv6" por parte de las administraciones públicas.
6. Promover la implantación de "IPv6" por parte de las asociaciones profesionales y empresariales.
7. Promover el uso de nuevas redes, servicios y aplicaciones "IPv6" en el sector público por parte de las administraciones públicas.
8. Explorar el impacto de "IPv6" en la provisión de seguridad extremo a extremo y auditoría de la información, así como de la protección de datos de carácter personal o privado.
9. Potenciar proyectos que permitan la explotación de dicho impacto mediante provisión de plataformas de seguridad en pilotos y redes emergentes de "IPv6".

Se expone el caso específico de España debido a que aunque son muchas las diferencias que tiene este país con Costa Rica se puede ver que las recomendaciones que se hacen al Ministerio de Ciencia y Tecnología Español y a las diferentes entidades

son (a excepción del punto 4) fácilmente aplicables a nuestro país, en el cual urge que se tomen iniciativas al respecto.

Además, en una segunda fase el "IPv6" task force español trabajará en la concreción de medidas orientadas al sector público y la industria.

La presentación completa donde se explica la iniciativa española se puede encontrar en http://www.spain.ipv6tf.org/public/ipv6TF_spain_v10.pdf, http://www.ec.ipv6tf.org.

6.8 El IPv6 forum

Fue constituido el 7 de julio de 1999 y según las palabras de Latif Ladid, Presidente del Foro IPv6, se define como un consorcio mundial de proveedores líderes de Internet, Redes de Educación e Investigación, con la clara misión de promocionar IPv6 al mejorar dramáticamente su reconocimiento por parte del mercado y los usuarios y al crear la Nueva Generación de Internet con calidad y seguridad y permitir el acceso equitativo mundial al conocimiento y la tecnología, abrazando una responsabilidad moral del mundo.

Para este fin, el Foro IPv6 deberá:

- Establecer un Foro internacional y abierto de experiencia en IPv6.
- Compartir los conocimientos y experiencias de IPv6 entre los miembros.
- Promocionar nuevas aplicaciones basadas en IPv6 y soluciones globales.
- Promocionar la interoperabilidad de implementaciones normalizadas de IPv6.
- Cooperar para alcanzar calidades de servicio extremo a extremo.
- Resolver problemas que creen barreras para el uso de IPv6.

El Foro IPv6 no desarrollará el protocolo, dado que la única autoridad competente para esta misión es el IETF (Internet Engineering Task Force).

- Algunos de los principales miembros del ipv6 forum son:

#	Empresa	#	Empresa
1	Case Technology, UAE	39	Centre for Wireless Communications, Singapore
2	Thomson CSF Detexis, France	40	Siemens, Germany
3	Ericsson Telebit, Denmark	41	IBM, USA
4	Eurocontrol, France	42	BellSouth, USA
5	Gigabell, Germany	43	Teleglobe, USA
6	Hitachi, Japan	44	Silicon Graphics, Inc (SGI), USA
7	Hewlett Packard, USA	45	Etisalat, UAE
8	DFN, Germany	46	SwitchCore AB, Sweden
9	Canarie Viagenie, Canada	47	UCAID Internet2, USA

10	NTT, Japan	48	University College of London (UCL), UK
11	WIDE, Japan	49	University of Southampton, United Kingdom
12	BT, UK	50	University of Lancaster, United Kingdom
13	CSELT, Italy	51	Royal Philips The Netherlands
14	Mentat, USA	52	Royal KPN (Royal Dutch Telecom) The Netherlands
15	SUN, USA	53	The Open Group UK
16	Netmedia, Finland	54	CIAC, France
17	Trumpet Software, Australia	55	UNINETT, Norway
18	Intracom, Greece	56	NEC, Japan
19	Cisco, USA	57	ETRI, Korea
20	COMPAQ, USA	58	INTAP, Japan
21	SPRINT, USA	59	Alpha Group, USA
22	NOKIA, USA	60	Korea Telecom, Korea
23	AT&T, USA	61	CNRS, France
24	Teldat, Spain	62	YDC (Yokogawa Digital Computer Corporation), Japan
25	Deutsche Telekom, Germany	63	Alcatel, France
26	Qwest, USA	64	GITEP, France
27	IABG, Germany	65	ISI, USA – UK
28	Esnet 6REN, USA	66	Nortel Networks
29	MCI WorldCom, USA	67	ISOC
30	Ericsson, Sweden	68	StardUSAt.com, USA
31	Microsoft, USA	69	Telefónica Spain
32	3Com, USA	70	Telscom, CH
33	Advanced Systems Consulting, Inc., USA	71	NFP, Finland
34	Consulintel, Spain	72	Lucent, EU/USA
35	The Bussiness Internet, USA	73	IMAG, France
36	NTT Software Corporation, Japan	74	France Telecom
37	Motorola, USA	75	Apple
38	Telia Networks Services, Sweden	76	SPAWAR

6.9 Implicaciones administrativas

Todo proceso de cambio acarrea implicaciones para la empresa las cuales deben tomarse en cuenta como información de apoyo al decidir sobre cómo y cuándo se va a ejecutar; como sucede en nuestro caso de estudio "El cambio de protocolo hacia "IPv6"".

IPV6, por su origen y naturaleza compatible con "IPv4", permite que la implantación sea menos impactante para las empresas. Sin embargo, toda implantación genera implicaciones administrativas de las cuales las más evidentes son las siguientes:

- Cada empresa, partiendo de su estado, deberá planear una estrategia de implantación.
- El personal técnico encargado de ejecutar el cambio debe ser capacitado para lograr la implantación.
- Según el estado del hardware y software de la empresa; este requerirá actualizaciones y cambios, lo que puede generar gastos en horas de personal y además inversiones; al tener que cambiar equipos o software que no soporte una actualización.
- En una implantación bien planteada y escalonada se evitará la contratación de personal adicional o compras masivas de equipo.
- Se debe crear conciencia entre el personal de la empresa de los beneficios que traerá consigo el cambio; sin embargo, se debe recalcar que se deben utilizar para beneficio de la organización; así mismo se debe identificar la manera de explotar esta optimización en las comunicaciones.
- Si se planifica adecuadamente la transición, no se incurrirá en gastos extras, ya que se está utilizando el equipo y software existente; en los casos que el software o equipos no soporten la actualización, sí será necesario reemplazarlos pero a largo o mediano plazo; por lo que prácticamente se podrá utilizar toda la vida útil del equipo.

6.10 Costo/Beneficio

En cuanto a los costos por adquisición del equipo, como se ha detallado anteriormente, si se planea adecuadamente la implantación no se incurrirá en compra masiva de equipos; debido a que se puede utilizar la mayoría durante su vida útil. En cuanto al software, la situación es la misma ya que mediante actualizaciones, mejoras de versiones y parches, se puede actualizar software para hacerlo compatible con IPv6; en caso de no poderse hacer una actualización se debe recordar que las redes IPv4 podrán interactuar con las IPv6.

Eventualmente se incurrirá en un costo del planeamiento y ejecución de la transición pero esto se puede establecer dentro del mantenimiento periódico que llevan los equipos de comunicaciones para su buen funcionamiento. De este modo los desembolsos de las empresas serán más pequeños y en plazos.

Se debe incurrir en una capacitación adecuada del personal para poder hacer la transición; sin embargo, esto se retribuirá a largo plazo con una mejora global en las comunicaciones de la empresa; y en la inversión en el capital intelectual.

Como se puede apreciar, los costos de una implantación bien planeada no obligará a inversiones gigantescas ni inmediatas; para lograr obtener la gran cantidad de beneficios que provee el nuevo protocolo de Internet.

Entre los beneficios principales que se obtendrán de la transición están:

- Optimización general de las comunicaciones.
- Mayor seguridad en las comunicaciones; características de IPsec intrínsecas en IPv6.
- Mayor agilidad y velocidad en las comunicaciones.
- Mayor espacio de direcciones (las empresas tendrán más opción a direcciones públicas)
- Se mantendrá a la empresa a la vanguardia de las comunicaciones, evitando el peligro futuro de aislarse por incompatibilidad.
- Dispositivos plug & play " auto-configuración "

- Posibilidad de manejar múltiples direcciones en los nodos e inclusive en las interfaces.
- Paquetes con mayor carga útil, libres de fragmentación.
- Movilidad.
- Escalabilidad de IPv6; que dice que permitirá migrar o actualizarse según las necesidades que se presenten en el futuro.

Si se observa bien, los beneficios obtenidos al migrar o evolucionar a IPv6 son muchos y a un bajo costo; ya que solo se debe ser visionarios y actualizar los equipos en cuanto a software y hardware; además si se debe adquirir equipos nuevos, en la mayoría ya se incorporan elementos de IPv6 por lo que solamente se debe estar atentos a los cambios que se presenten y tener en mente que cualquier cambio en las redes debe ser contemplando la futura migración a IPv6.

6.11 Apoyo de las grandes empresas a IPv6

La cantidad de empresas que se están sumando al esfuerzo mundial del IPv6 es cada vez mayor; por ejemplo gigantes de la industria de las comunicaciones ya forman parte de los miembros del "l Foro IPv6 "; además muchas ya hacen público su compromiso; como por ejemplo:

Cisco Systems

En junio del 2000, Cisco Systems anunció su estrategia hacia IPv6; esta consistía de 3 fases según lo descrito en la declaración del IOS IPv6 del Cisco.
En mayo del 2001 ya se tenía a disponibilidad las características IPv6 en software del Cisco IOS®; hoy en día se encuentra en progreso la fase III con una nueva versión del IOS IPv6 Cisco y algunas implementaciones como por ejemplo OSPFv3, IPv6 QoS, DHCPv6, el multicast IPv6, NAT-PT.
Algunos productos son los siguientes:

- Cisco 3640, Cisco 2621, y Cisco 7507 series routers.
- Cisco IOS Software (C3640-IS-M), Versión 12.2(8)T4.
- Cisco IOS Software (C2600-IS-M), Versión 12.2(8)T4.
- Cisco IOS RSP Software (RSP-IK9SV-M), Versión 12.2(8)T4.

3com

3Com ha sido un partidario temprano de la iniciativa IPv6 y es un miembro fundador del foro IPv6. Propone completamente proporcionar respuestas sólidas y puestas en práctica que sean de forma estándar, simples, y rentables. Después de la trayectoria del despliegue actual, introducirá inicialmente características IPv6 en los routers WAN. El paso siguiente incluirá una línea de productos modular para la empresa grande.
Según indica un encargado de prensa de la compañía " En un cierto plazo los productos de los 3Com convergerán a IPv6. Porque entendemos las necesidades de nuestros usuarios, proporcionaremos las herramientas eficaces para ayudar a la transición".

Linux

Linux no ha sido la excepción y para citar un ejemplo está el "Linux IP v6 users group" ; que existe desde 1998. Entre otros proyectos tienen la creación de actualizaciones de software o parches que ponen a la disponibilidad de los usuarios de linux en diferentes sitios de forma gratuita los cuales permiten la interoperabilidad con ipv6. La dirección del sitio es http://www.v6.linux.or.jp/.
Un ejemplo de esto es el artículo http://www.linuxjournal.com/article.php?sid=4763; que trata del soporte a IPv6 en un servidor de linux.

Solaris

Para " Sun y Solaris", el soporte a las redes IPv6 es una clara prioridad. Con el lanzamiento del ambiente de funcionamiento de Solaris 8 en febrero del 2000, Sun ofrece el apoyo total para los protocolos de red IPv6 e IPv4. Los ingenieros de la empresa y los socios comerciales están probando ahora las mejoras que se harán para soportar la próxima generación del protocolo de Internet. Solaris participa activamente en la IETF con respecto al protocolo IPv6, y su código se ha estado probando por más

de cinco años. Este esfuerzo del desarrollo rindió una puesta en práctica del primer prototipo que estaba disponible en 1995. Sun entrega el establecimiento de una red IPv6 en el último lanzamiento de Solaris como parte integral de su estrategia para la nueva era de Internet. El Internet ha servido como base vital en permitir comunicaciones electrónicas y compartir información. Para continuar proporcionando esto, necesita crecer y desarrollarse -- sin interrupción -- para apoyar el aumento de usuarios. Esto ha sido una fuerza impulsora dominante detrás del desarrollo del IPv6. En el pasado, el papel de el Internet también se ha desarrollado para convertirse en un medio de comunicaciones crítico del negocio.

Microsoft

En la actualidad, Microsoft dispone del software IPv6 Technology Preview, que funciona sobre Windows 2000 SP1 y puede ser descargado desde la sede MSDN (http://msdn.microsoft.com/downloads/sdks/platform/tpipv6.asp). Este programa es una pila IPv6 para Windows 2000 para desarrolladores, y constituye el segundo paso de los cuatro de que constaba la estrategia de Microsoft.

En el caso de Windows XP, la versión beta 2 ya incluía IPv6 en el propio sistema operativo.

En la actualidad, Microsoft incluye las siguientes aplicaciones que funcionan sobre IPv6:

- Utilidades de red: ping6, tracert6 (traceroute para IPv6) y ttcp (programa para probar la conexión TCP entre dos máquinas).
- Internet Explorer.
- Los clientes de FTP y Telnet (telnet.exe y ftp.exe) son capaces de conectarse a servidores IPv6.
- Servidor Telnet: el servidor de Telnet de Microsoft permite de establecer sesiones telnet con clientes IPv4 y IPv6.
- Programas que utilizan RPC ("Remote Procedure Calls" o Llamadas de procedimiento remoto) y pueden ejecutarse sobre IPv6 ya desde la beta 1 de Windows XP. Hay desarrolladores que ya trabajan con IPv6. En la dirección

http://win6.goto.info.waseda.ac.jp pueden encontrarse algunas aplicaciones que funcionan en Windows con IPv6 (desde un servidor web de Apache hasta versiones del sniffer de red Windump).

Además de la implementación de Microsoft, la compañía Trumpet, pionera en la creación de una pila TCP/IP para Windows, ha desarrollado su propia pila IPv6 para Windows 95/98/NT. La pila y más información sobre la misma están disponibles en la dirección web www.trumpet.com.au/ipv6.htm.

6.12 Recurso Humano

En realidad para la transición de IPv4 a IPv6; no se necesita recursos humanos específicos en esa área, de manera que los técnicos o soportistas con un poco de capacitación podrían configurar los equipos para esta tarea. Además es aconsejable que sea el mismo personal de la empresa el que se capacite para hacer el cambio ya que este personal deberá dar mantenimiento en el futuro a esta plataforma.
De manera que en cuanto a recurso humano los requerimientos o requisitos necesarios serían básicamente los mismos de la actualidad, eso sí estos técnicos o soportistas deberán ser de soporte avanzado, ya que este personal está acostumbrado a resolver problemas de conectividad y configuración de equipos de red, servidores y pc´s.
Entre los mas importantes tenemos :

- Instalar y coadyuvar a la configuración de servidores, equipos de comunicaciones, aplicaciones y estaciones de trabajo para ser utilizadas por los funcionarios de la empresa.

- Monitorear el funcionamiento de sistemas de información, preparar los reportes de asistencia técnica para la atención de problemas indicados por los funcionarios con respecto a mensajes de error en sistemas de información. Notificar y resolver en forma inmediata cualquier problema que suspenda parcial o totalmente el funcionamiento de los sistemas.

- Monitorear el funcionamiento de hardware principal del centro de cómputo y notificar de cualquier mensaje de error. Notificar y resolver en buena forma cualquier problema con el hardware principal que suspenda parcial o totalmente el funcionamiento de los sistemas.

- Monitorear o detectar problemas con las comunicaciones para realizar reportes de averías.

- Coadyuvar en la instalación o cambio de cableado de red para las estaciones de trabajo.

- Realizar mantenimiento preventivo o correctivo básico al hardware y software de las estaciones de trabajo o coordinar con el proveedor del servicio la atención de las averías.

- Efectuar y controlar los procesos de carga de información en los sistemas de Información.

- Conocer la metodología de respaldo y ejecutar los procesos de respaldo de información. Llevar su registro y control. Coordinar con el área de Sistemas la verificación de la información de los respaldos y prueba.

- Realizar procesos de capacitación básica sobre herramientas de oficina.

- Brindar soporte en la eliminación de virus y mantener actualizadas las versiones de los antivirus.

- Participar en la realización de estudios técnicos, que respalden la labor de Profesionales.
- Controlar el uso correcto del equipo asignado a los funcionarios verificando que se cumplan las políticas emitidas en esa materia.

- Contribuir en las acciones que se desarrollen para garantizar el correcto funcionamiento de los sistemas y equipos de cómputo y así obtener una adecuada y oportuna utilización de la información.

- Llevar el control de ingresos de personas al centro de cómputo. Coordinar el ingreso del personal autorizado para realizar labores de mantenimiento preventivo o correctivo a los diversos equipos.

- Llevar el control de activos del equipo de cómputo de su unidad organizativa, por medio de números de activo, marca de equipo y otros, con el objeto de conocer y reportar las deficiencias.

- Coadyuvar con la notificación de la suspensión temporal de redes o sistemas a los usuarios internos y externos para realizar labores de mantenimiento preventivo o correctivo o cambios de sistemas.

- Ejecutar cualquier otra actividad técnica correspondiente a los diversos procesos informáticos que se ejecutan que sea asignada por la Jefatura de Informática

- En general coadyuvar a vigilar el cumplimiento de las políticas que se emitan en materia informática.

- Es deseable que quien ocupe este tipo de puestos posea capacidad analítica, capacidad de trabajo en equipo y habilidad para coordinar actividades, capacidad de aprendizaje, con una gran identificación con los objetivos institucionales y de su unidad, facilidad para formular y aceptar críticas, así como para propiciar el intercambio de ideas entre personal de diversas disciplinas, ser organizado y disciplinado en los métodos de trabajo.

- Su trabajo requiere de gran capacidad de concentración y análisis, dada la importancia de su accionar y lo extenso de su ámbito de trabajo.

- Debe poseer capacidad para transferir conocimientos y buena disposición al cambio.

6.13 Capacitación específica en cuanto a IPv6

Como en nuestro país no se conoce ninguna capacitación específica en este tema, el soportista debe ser autodidacta para poder leer, comprender y aplicar configuraciones y especificaciones que se encuentran en manuales técnicos y manuales de instalación. Además, esta tarea permite capacitar y familiarizar al personal con el nuevo protocolo el cual se convertirá sin duda en el futuro en una herramienta de trabajo diario.

Bibliografía

Bibliografía Citada

Hernández, Roberto. (1991) Metodología de la Investigación. Editorial MacGraw-Hill, Méjico.

Arellano Galdames, F. Jaime (1987) Elementos de Investigación: La investigación a través de su informe. Octava Reimpresión, San José, Costa Rica EUNED

7.2 Bibliografía Consultada

Arellano Galdames, F. Jaime (1987) Elementos de Investigación: La investigación a través de su informe. Octava Reimpresión, San José, Costa Rica EUNED

James A Senn, (1.993) Análisis y Diseño de Sistemas de Información, 2. ed. México: McGRAW-HILL INTERAMERICANA DE MEXICO, S.A. de CV.

Hernández, Roberto. (1.991) Metodología de la Investigación. Editorial MacGraw-Hill Méjico.

Fernández, César. (1.998) Metodología de la Investigación, Costa Rica.

Stephen Thomas. (1.996) Ipng and the TCP/IP Protocols, Wiley.

Habraken ,Joe . (2000) Routers Cisco , Prentice Hall ,Madrid

Cysco Systems Inc. (2002) Academia de Networking de Cisco Systems : Guia del Primer Año ,Pearson Education , Madrid

Cysco Systems Inc. (2002) Academia de Networking de Cisco Systems : Guia del Segundo Año ,Pearson Education , Madrid

RFC's

RFC2460, Especificaciones del Protocolo Internet Versión 6 (IPv6)

RFC2462, Autoconfiguración de Direcciones "stateless" IPv6

RFC2463, Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)

RFC2373, Arquitectura de Direccionamiento en IPv6

RFC1887, Arquitectura para la Asignación de Direcciones Unicast IPv6

RFC2374, Formato de Direcciones Unicast Agregables Globales

RFC2464, Transmisión de paquetes IPv6 sobre redes Ethernet

RFC2401, Arquitectura de Seguridad para IP

RFC2526, Direcciones de Subredes para Anycast en IPv6

RFC2185, Aspectos de Routing de la Transición IPv6

RFC2473, Especificaciones Genéricas de Tunelización de Paquetes en IPv6

RFC2529, Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos

RFC1924, Representación Compacta de Direcciones IPv6

RFC2732, Formato para la representación literal de direcciones IPv6 en URL's

7.3 Direcciones de Int ernet

http://www.ipv6forum.com/

http://www.6bone.net/

http://www.6ren.net/

http://www.ipv6.org/

http://www.microsoft.com

http://lat.3com.com/lat/

http://www.cisco.com/

www.ipv6.unam.mx

www .trumpet.com.au/ipv6.htm

http://www.spain.ipv6tf.org/public/ipv6TF_spain_v10.pdf

http://www.ec.ipv6tf.org.

Anexos

CUESTIONARIO

De antemano le agradecemos el tomar unos minutos de su valioso tiempo para contestar el siguiente cuestionario el cual tiene como objeto diagnosticar aspectos importantes con respecto al tema **" Hacia la siguiente g eneración del Protocolo de Internet "**, esto como parte de un trabajo de investigación presentado como proyecto de graduación en la carrera de Lic. informática en Ulacit.

Le aseguramos la absoluta confidencialidad de la información brindada.

INSTRUCCIONES: MARQUE CON UNA X SOBRE EL NÚMERO CORRESPONDIENTE AL NIVEL DE CONOCIMIENTO SEGÚN CORRESPONDA EN LA ESCALA DEL 1 AL 10 DONDE 1 ES NADA Y 10 ES MUCHO. O RESPONDA SI O NO SEGÚN SEA EL CASO.

1 ¿Cuánto conoce usted acerca del protocolo de Internet "IP"?

nada 1 2 3 4 5 6 7 8 9 10 mucho

2 ¿Sabe usted cuál es la versión de "IP" que se utiliza actualmente?

Sí □ Cuál_____ No □

3 ¿Tiene usted algún conocimiento de la siguiente generación del protocolo de Internet?

nada 1 2 3 4 5 6 7 8 9 10 mucho

4 ¿Cuánto conoce usted acerca de IPv4?

nada 1 2 3 4 5 6 7 8 9 10 mucho

5 ¿Tiene usted algún conocimiento de la IPv6?

nada 1 2 3 4 5 6 7 8 9 10 mucho

6 ¿Cuánto conoce usted acerca de IPv6?

nada 1 2 3 4 5 6 7 8 9 10 mucho

7 ¿Conoce usted algunas diferencias entre IPv4 e IPv6?

Sí □ No □

Podría definir 3

1._____.
2._____.
3._____.

7 ¿Cree usted que el cambio de IPv4 a IPv6 traerá algún beneficio?

Sí □ Cuál_____ No □

9 ¿Conoce usted las tendencias actuales del hardware de comunicaciones en cuanto a direccionamiento de datos?

nada mucho
1 2 3 4 5 6 7 8 9 10

10 ¿Conoce usted las tendencias actuales del software de los equipos de comunicación en cuanto a direccionamiento?

nada mucho
1 2 3 4 5 6 7 8 9 10

11 ¿Conoce usted algún equipo (hardware) del mercado que sea compatible con IPv6?

Sí □ Cuál_____ No □

12 ¿Conoce usted algún software del mercado que sea compatible con IPv6?

Sí □ Cuál_____ No □

13 ¿Tiene usted idea de cuál será el costo/beneficio de hacer el cambio de protocolo?

Sí □ No □

14 ¿Sabe usted acerca de las características del recurso humano necesario para enfrentar el cambio de versión del protocolo de Internet a IPv6?

Sí □ No □

Podría definir 3 características

1._____.
2._____.
3._____.

15 ¿Sabe usted qué implicaciones administrativas va a generar el cambio de protocolo a IPv6?

Sí □ No □

16 ¿Conoce usted alguna documentación actualizada que le pudiese ayudar a efectuar el cambio?

Sí □ Cuál_____ No □

17 ¿Cómo país (Costa Rica) cómo cree usted que se le ha dado la importancia necesaria al tema "Cambio de versión del protocolo de Internet de IPv4 a IPv6"?

nada mucho

1 2 3 4 5 6 7 8 9 10

18 ¿Ha recibido usted de alguna entidad (Universidad, Colegio profesional u otro) Alguna información al respecto?

Sí □ Cuál_____ No □

19 ¿Desea usted expresar alguna inquietud con respecto a este tema?

Gracias.

DECLARACIÓN JURADA

Yo Randall Hernández Solano alumno de La Unversidad de Ciencia Y Tecnología (Ulacit) , declaro bajo la fé de juramento y consciente de la responsabilidad penal de este acto, que soy el autor intelectual de la tesis de grado titulada "**Hacia la siguiente generación del Protocolo de Internet ",** por lo que libreo a Ulacit , de cualquier responsabilidad en caso de que mi declaración sea falsa.

Brindada en San José – Costa Rica en el día 01 del mes de diciembre del año dos mil cuatro.

Firma:_____ Cédula de Identidad :_____.

ULACIT

UNIVERSIDAD LATINOAMERICANA DE CIENCIA Y TECNOLOGÍA

TRIBUNAL EXAMINADOR

Reunido para los efectos respectivos, el Tribunal Examinador de la Escuela de Postgrados compuesto por:

Tutor

Lector

Presidente del Tribunal

Apéndices

Apéndice 1

Tutorial de IPV4

Tutorial de ipv4

El protocolo de Internet; "Ipv4"

El Protocolo Internet está diseñado para su uso en sistemas interconectados de redes de comunicación de ordenadores por intercambio de paquetes. El protocolo Internet proporciona los medios necesarios para la transmisión de bloques de datos llamados datagramas desde el origen al destino, donde origen y destino son hosts identificados por direcciones de longitud fija. El protocolo Internet también se encarga, si es necesario, de la fragmentación y el reensamblaje de grandes datagramas para su transmisión a través de redes de trama pequeña.
IP es un sistema no orientado a la conexión, que maneja cada paquete de forma independiente. Por ejemplo, si se usa un programa FTP para descargar un archivo, IP no envía el archivo en una larga cadena de datos. IP maneja cada paquete de forma independiente. Cada paquete puede viajar a través de distintas rutas. Algunos paquetes incluso pueden perderse. IP se basa en el protocolo de la capa de transporte para determinar si los paquetes se han perdido y para solicitar que se vuelvan a transmitir. La capa de transporte también tiene la responsabilidad de colocar los paquetes nuevamente en el orden correcto.

Ámbito

El Protocolo Internet está específicamente limitado a proporcionar las funciones necesarias para enviar un paquete de bits (un datagrama Internet) desde un origen a un destino a través de un sistema de redes interconectadas. No existen mecanismos para aumentar la fiabilidad de datos entre los extremos, control de flujo, secuenciamiento u otros servicios que se encuentran normalmente en otros protocolos host-a-host. El protocolo Internet puede aprovecharse de los servicios de sus redes de soporte para proporcionar varios tipos y calidades de servicio.

Operación

El protocolo Internet implementa dos funciones básicas:

Direccionamiento y Fragmentación.

Los módulos Internet usan las direcciones que se encuentran en la cabecera Internet para transmitir los datagramas Internet hacia sus destinos. La selección de un camino para la transmisión se llama enrutamiento.

Los módulos Internet usan campos en la cabecera Internet para fragmentar y reensamblar los datagramas Internet cuando sea necesario para su transmisión a través de redes de "trama pequeña".

El modelo de operación es que un módulo Internet reside en cada host involucrado en la comunicación Internet y en cada pasarela que interconecta redes. Estos módulos comparten reglas comunes para interpretar los campos de dirección y para fragmentar y ensamblar

datagramas Internet. Además, estos módulos (especialmente en las pasarelas) tienen procedimientos para tomar decisiones de enrutamiento y otras funciones.

El protocolo Internet trata cada datagrama Internet como una entidad independiente no relacionada con ningún otro datagrama Internet. No existen conexiones o circuitos lógicos (virtuales o de cualquier otro tipo).

El protocolo Internet utiliza cuatro mecanismos clave para prestar su servicio: Tipo de Servicio, Tiempo de Vida, Opciones, y Suma de Control de Cabecera.

El Tipo de Servicio se utiliza para indicar la calidad del servicio deseado. El tipo de servicio es un conjunto abstracto o generalizado de parámetros que caracterizan las elecciones de servicio presentes en las redes que forman Internet. Esta indicación de tipo de servicio será usada por las pasarelas para seleccionar los parámetros de transmisión efectivos para una red en particular, la red que se utilizará para el siguiente salto, o la siguiente pasarela al encaminar un datagrama Internet.

El Tiempo de Vida es una indicación de un límite superior en el periodo de vida de un datagrama Internet. Es fijado por el remitente del datagrama y reducido en los puntos a lo largo de la ruta donde es procesado. Si el tiempo de vida se reduce a cero antes de que el datagrama llegue a su destino, el datagrama Internet es destruído.
Puede pensarse en el tiempo d e vida como en un plazo de autodestrucción.
Las Opciones proporcionan funciones de control necesarias o útiles en algunas situaciones pero innecesarias para las comunicaciones más comunes. Las opciones incluyen recursos para marcas de tiempo, seguridad y enrutamiento especial.

La Suma de Control de Cabecera proporciona una verificación de que la información utilizada al procesar el datagrama Internet ha sido transmitida correctamente. Los datos pueden contener errores. Si la suma de control de cabecera falla, el datagrama Internet es descartado inmediatamente por la entidad que detecta el error.
El protocolo Internet no proporciona ningún mecanismo de comunicación fiable. No existen acuses de recibo ni entre extremos ni entre saltos.
No hay control de errores para los datos, sólo una suma de control de cabecera. No hay retransmisiones. No existe control de flujo.

Protocolos TCP/IP de Internet

El conjunto de protocolos Protocolo de Control de Transmisión / protocolo Internet (TCP/IP) se desarrolló como parte de la investigación realizada por la Agencia de Proyectos de Investigación Avanzada para la Defensa (DARPA). Originalmente, se desarrolló para suministrar comunicaciones a través de DARPA. Posteriormente, TCP/IP se incluyó en la Distribución del Software Berkeley de UNIX. TCP/IP es hoy el estándar de facto para las comunicaciones de ¨Internetwork ¨ y sirve como el protocolo de transporte para Internet, permitiendo que millones de computadores se comuniquen a nivel mundial.

TCP/IP permite la comunicación entre cualquier conjunto de redes interconectadas y sirve tanto para las comunicaciones de LAN como de WAN.

IP : suministra enrutamiento de datagramas no orientado a conexión, de máximo esfuerzo de entrega; no se ocupa del contenido de los datagramas; busca la forma de desplazar los datagramas al destino

TCP : un protocolo confiable, orientado a conexión; suministra control de flujo a través de ventanas deslizantes, y confiabilidad a través de los números de secuencia y acuses de recibo. TCP vuelve a enviar cualquier mensaje que no se reciba y suministra un circuito virtual entre las aplicaciones del usuario final. La ventaja de TCP es que proporciona una entrega garantizada de los segmentos.

Propósito de las direcciones IP

En un entorno TCP/IP, las estaciones finales se comunican con servidores u otras estaciones finales. Esto puede ocurrir porque cada nodo que utiliza el conjunto de protocolo TCP/IP tiene una dirección lógica exclusiva de 32 bits. Esta dirección se denomina dirección IP y se especifica en formato decimal separado por puntos de 32 bits. Las interfaces del router se deben configurar con una dirección IP si IP se debe enrutar hacia o desde la interfaz.

Descripción de Funciones

La función o propósito del Protocolo Internet es mover datagramas a través de un conjunto de redes interconectadas. Esto se consigue pasando los datagramas desde un módulo Internet a otro hasta que se alcanza el destino. Los módulos Internet residen en hosts y pasarelas en el sistema Internet. Los datagramas son encaminados desde un módulo Internet a otro a través de redes individuales basándose en la interpretación de una dirección Internet. Por eso, un importante mecanismo del protocolo Internet es la dirección Internet.

En el enrutamiento de mensajes desde un módulo Internet a otro, los datagramas pueden necesitar atravesar una red cuyo tamaño máximo de paquete es menor que el tamaño del datagrama. Para salvar esta dificultad se proporciona un mecanismo de fragmentación en el protocolo Internet.

Direccionamiento

Se establece una distinción entre nombres, direcciones y rutas.
Un nombre indica qué buscamos.
Una dirección indica dónde está.
Una ruta indica cómo llegar allí.

El protocolo Internet maneja principalmente direcciones. Es tarea de los protocolos de mayor nivel (es decir, protocolos host-a-host o entre aplicaciones) hacer corresponder nombres con

direcciones. El módulo Internet hace corresponder direcciones de Internet con direcciones de red local. Es tarea de los procedimientos de menor nivel (es decir, redes locales o pasarelas) realizar la correspondencia entre direcciones de red local y rutas.

Las direcciones son de una longitud fija de 4 octetos (32 bits). Una dirección comienza por un número de red, seguido de la dirección local (llamada el campo "resto"). Hay 3 formatos o clases de direcciones Internet: En la Clase A, el bit más significativo es 0, los 7 bits siguientes son la red, y los 24 bits restantes son la dirección local; en la Clase B, los dos bits más significativos son uno-cero ("10"), los 14 bits siguientes son la red y los últimos 16 bits son la dirección local; en la Clase C, los tres bits más significativos son uno-uno-cero ("110"), los 21 bits siguientes son la red y los 8 restantes son la dirección local.

Se debe tener cuidado al relacionar direcciones Internet con direcciones de red local; un host individual físicamente hablando debe ser capaz de actuar como si fuera varios hosts distintos, hasta el punto de usar varias direcciones Internet distintas. Algunos hosts tendrán también varios interfaces físicos.

Fragmentación

La fragmentación de un datagrama Internet es necesaria cuando éste se origina en una red local que permite un tamaño de paquete grande y debe atravesar una red local que limita los paquetes a un tamaño inferior para llegar a su destino.

Un datagrama Internet puede ser marcado como "no fragmentar". Todo datagrama Internet así marcado no será fragmentado entre distintas redes bajo ninguna circunstancia. Si un datagrama Internet marcado como "no fragmentar" no puede ser entregado en su destino sin fragmentarlo, entonces debe ser descartado.

La fragmentación, transmisión y reensamblaje a través de una red local invisible para el módulo del protocolo Internet se llama fragmentación intranet y puede ser utilizada .
El procedimiento de fragmentación y reensamblaje en Internet tiene que ser capaz de dividir un datagrama en un número casi arbitrario de piezas que puedan ser luego reensambladas. El receptor de los fragmentos utiliza el campo de identificación para asegurarse de que no se mezclan fragmentos de distintos datagramas. El campo posición ("offset") le indica al **receptor** la posición de un fragmento en el datagrama original. La posición y longitud del fragmento determinan la porción de datagrama original comprendida en este fragmento. El indicador "más-fragmentos" indica (puesto a cero) el último fragmento. Estos campos proporcionan información suficiente para reensamblar datagramas.
El campo identificador se usa para distinguir los fragmentos de un datagrama de los de otro. El módulo de protocolo de origen de un datagrama Internet establece el campo identificador a un valor que debe ser único para ese protocolo y par origen-destino durante el tiempo que el datagrama estará activo en el sistema Internet. El módulo de protocolo de origen de un datagrama completo pone el indicador "más-fragmentos" a cero y la posición del fragmento a cero.
Para fragmentar un datagrama Internet grande, un módulo de protocolo Internet (por ej.: en una pasarela) crea dos nuevos datagramas Internet y copia el contenido de los campos de cabecera Internet del datagrama grande en las dos cabeceras nuevas. Los datos del datagrama grande son divididos en dos trozos tomando una resolución mínima de 8 octetos (64 bits) (el segundo trozo

puede no ser un múltiplo entero de 8 octetos, pero el primero sí debe serlo). Llamemos al número de bloques de 8 octetos en el primer trozo NFB
(Number of Fragment Blocks: Número de Bloques del Fragmento). El primer trozo de datos es colocado en el primer nuevo datagrama Internet y el campo longitud total se establece a la longitud del primer datagrama. El indicador "más-fragmentos" indica (puesto a cero) el último fragmento. Estos campos proporcionan información suficiente para reensamblar datagramas.

El campo identificador se usa para distinguir los fragmentos de un datagrama de los de otro. El módulo de protocolo de origen de un datagrama Internet establece el campo identificador a un valor que debe ser único para ese protocolo y par origen-destino durante el tiempo que el datagrama estará activo en el sistema Internet. El módulo de protocolo de origen de un datagrama completo pone el indicador "más-fragmentos" a cero y la posición del fragmento a cero.
Para fragmentar un datagrama Internet grande, un módulo de protocolo Internet (por ej.: en una pasarela) crea dos nuevos datagramas Internet y copia el contenido de los campos de cabecera Internet del datagrama grande en las dos cabeceras nuevas. Los datos del datagrama grande son divididos en dos trozos tomando una resolución mínima de 8 octetos (64 bits) (el segundo trozo puede no ser un múltiplo entero de 8 octetos, pero el primero sí debe serlo).
Llamemos al número de bloques de 8 octetos en el primer trozo NFB (Number of Fragment Blocks: Número de Bloques del Fragmento). El primer trozo de datos es colocado en el primer nuevo datagrama Internet y el campo longitud total se establece a la longitud del primer datagrama. El indicador "más fragmentos" es puesto a uno. El segundo trozo de datos es colocado en el segundo nuevo datagrama Internet y el campo longitud total se establece a la longitud del
segundo datagrama. El indicador "más fragmentos" lleva el mismo valor que en el datagrama grande. El campo posición del segundo nuevo datagrama se establece al valor de ese campo en el datagrama grande más NFB.

Este procedimiento puede generalizarse para una n-partición, mejor que para la división en dos partes descrita.

Para ensamblar los fragmentos de un datagrama Internet, un módulo de protocolo Internet (por ejemplo en un host de destino) combina todos los datagramas Internet que tengan el mismo valor en los cuatro campos: identificación, origen, destino y protocolo. La combinación se realiza colocando el trozo de datos de cada fragmento en su posición relativa indicada por la posición del fragmento en la cabecera Internet de ese fragmento. El primer fragmento tendrá posición cero, y el último fragmento tendrá el indicador "más fragmentos" puesto a cero.

Formato de la Cabecera Internet

A continuación vemos un resumen del contenido de la cabecera Internet.

El paquete IP está formado por los datos de las capas superiores más el encabezado IP, que está formado por:

- Versión: Indica la versión de IP que se usa en el momento (4 bits)

- Longitud del encabezado IP (HLEN): Indica la longitud del encabezado del datagrama en palabras de 32 bits (4 bits)
- Tipo de servicio: Especifica el nivel de importancia que le ha sido asignado por un protocolo de capa superior en particular (8 bits)
- Longitud total: Especifica la longitud de todo el paquete IP, incluyendo datos y encabezado, en bytes (16 bits)
- Identificación: Contiene un número entero que identifica el datagrama actual (16 bits)
- Señaladores: Un campo de 3 bits en el que los dos bits de orden inferior controlan la fragmentación; un bit que especifica si el paquete puede fragmentarse y el segundo si el paquete es el último fragmento en una serie de paquetes fragmentados (3 bits)
- Compensación de fragmentos: El campo que se utiliza para ayudar a reunir los fragmentos de datagramas (16 bits)
- Tiempo de existencia: Mantiene un contador cuyo valor decrece, por incrementos, hasta cero. Cuando se llega a ese punto se descarta el datagrama, impidiendo así que los paquetes entren en un loop interminable (8 bits)
- Protocolo: Indica cuál es el protocolo de capa superior que recibe los paquetes entrantes después de que se ha completado el procesamiento IP (8 bits)
- Suma de comprobación del encabezado: Ayuda a garantizar la integridad del encabezado IP (16 bits)
- Dirección origen: Especifica el nodo emisor (32 bits)
- Dirección destino: Especifica el nodo receptor (32 bits)
- Opciones: Permite que IP soporte varias opciones, como la seguridad (longitud variable)
- Datos: Contiene información de capa superior (longitud variable, máximo 64 kb)

Relleno: se agregan ceros adicionales a este campo para garantizar que el encabezado IP siempre sea un múltiplo de 32 bits

Campos origen y destino del encabezado IP

La dirección IP contiene la información necesaria para enrutar un paquete a través de la red. Cada dirección origen y destino contiene una dirección de 32 bits. El campo de dirección origen contiene la dirección IP del dispositivo que envía el paquete. El campo destino contiene la dirección IP del dispositivo que recibe el paquete.

Direcciones IP como un número binario de 32 bits

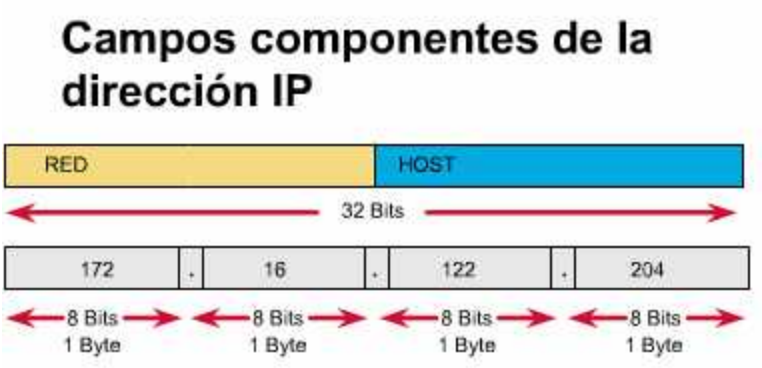
Una dirección IP se representa mediante un número binario de 32 bits. Como breve repaso, recuerde que cada dígito binario solo puede ser 0 ó 1. En un número binario, el valor del bit ubicado más a la derecha (también denominado bit menos significativo) es 0 ó 1. El valor decimal correspondiente para cada bit se duplica cada vez que avanza una posición hacia la izquierda del número binario. De modo que el valor decimal del 2do bit desde la derecha es 0 ó 2. El tercer bit es 0 ó 4, el cuarto bit 0 u 8, etc. ...

Las direcciones IP se expresan como números de notación decimal: se dividen los 32 bits de la dirección en cuatro *octetos* (un octeto es un grupo de 8 bits). El valor decimal máximo de cada octeto es 255 (el número binario de 8 bits más alto es 11111111, y esos bits, de derecha a izquierda, tienen valores decimales de 1, 2, 4, 8, 16, 32, 64 y 128, lo que suma 255 en total).

¿Cuál es el valor decimal del octeto que aparece resaltado en el gráfico? ¿Cuál es el valor del bit del extremo izquierdo? ¿El siguiente bit? Como estos son los únicos 2 bits que están activados (o establecidos), el valor decimal es 128+64=192

Campos que componen la dirección IP

El número de red de una dirección IP identifica la red a la que se conecta un dispositivo, mientras que la parte de una dirección IP que corresponde al host identifica el dispositivo específico de esa red. Como las direcciones IP están formadas por cuatro octetos separados por puntos, se pueden utilizar uno, dos o tres de estos octetos para identificar el número de red. De modo similar, se pueden utilizar hasta tres de estos octetos para identificar la parte del host de una dirección IP.



Clases de dirección IP

Hay tres clases de direcciones IP que una organización puede recibir de parte del Registro Estadounidense de Números de Internet (ARIN) (o ISP de la organización): Clase A, B y C. En la actualidad, ARIN reserva las direcciones de Clase A para los gobiernos de todo el mundo (aunque en el pasado se le hayan otorgado a empresas de gran envergadura como, por ejemplo, Hewlett Packard y las direcciones de Clase B para las medianas empresas. Se otorgan direcciones de Clase C para todos los demás solicitantes.

Clase A

Cuando está escrito en formato binario, el primer bit (el bit que está ubicado más a la izquierda) de la dirección de Clase A siempre es 0. Un ejemplo de una dirección IP de clase A es 124.95.44.15. El primer octeto, 124, identifica el número de red asignado por ARIN. Los administradores internos de la red asignan los 24 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red de Clase A es verificar el primer octeto de su dirección IP, cuyo valor debe estar entre 0 y 126. (127 *comienza* con un bit 0, pero está reservado para fines especiales).

Todas las direcciones IP de Clase A utilizan solamente los primeros 8 bits para identificar la parte de la red de la dirección. Los tres octetos restantes se pueden utilizar para la parte del host de la dirección. A cada una de las redes que utilizan una dirección IP de Clase A se les pueden asignar hasta 2 elevado a la 24 potencia (224) (menos 2), o 16.777.214 direcciones IP posibles para los dispositivos que están conectados a la red. 2

Clase B

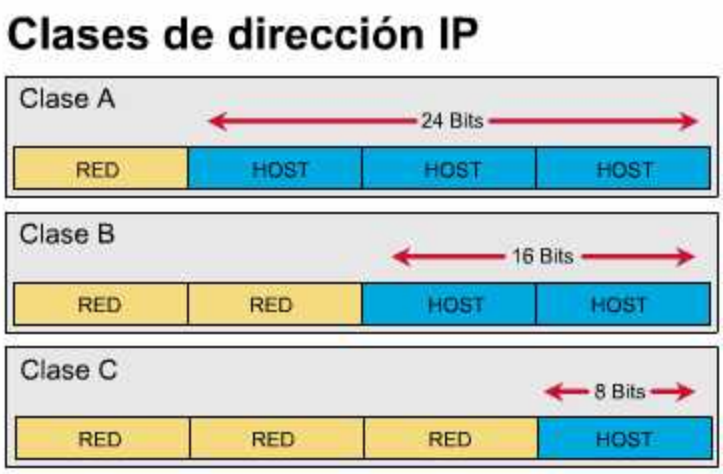
Los primeros 2 bits de una dirección de Clase B siempre son 10 (uno y cero). Un ejemplo de una dirección IP de Clase B es 151.10.13.28. Los dos primeros octetos identifican el número de red asignado por ARIN. Los administradores internos de la red asignan los 16 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red de Clase B es verificar el primer octeto de su dirección IP. Las direcciones IP de Clase B siempre tienen valores que van del 128 al 191 en su primer octeto.

Todas las direcciones IP de Clase B utilizan los primeros 16 bits para identificar la parte de la red de la dirección. Los dos octetos restantes de la dirección IP se encuentran reservados para la porción del host de la dirección. Cada red que usa un esquema de direccionamiento IP de Clase B puede tener asignadas hasta 2 a la 16ta potencia (216) (menos 2 otra vez), o 65.534 direcciones IP posibles a dispositivos conectados a su red.

Clase C

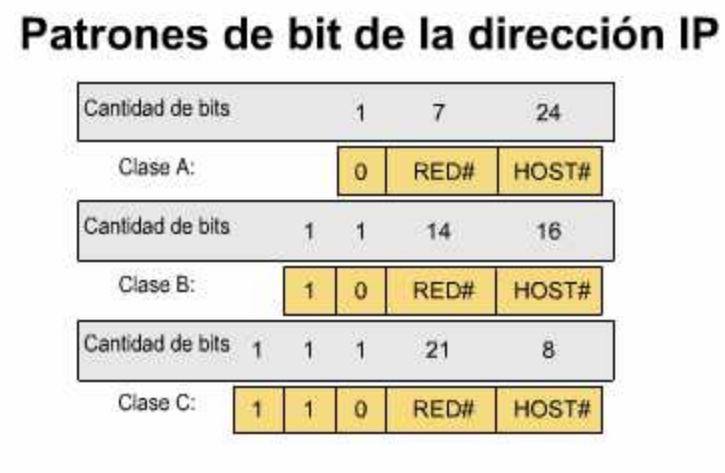
Los 3 primeros bits de una dirección de Clase C siempre son 110 (uno, uno y cero). Un ejemplo de dirección IP de Clase C es 201.110.213.28. Los tres primeros octetos identifican el número de red asignado por ARIN. Los administradores internos de la red asignan los 8 bits restantes. Una manera fácil de reconocer si un dispositivo forma parte de una red de Clase C es verificar el primer octeto de su dirección IP. Las direcciones IP de Clase C siempre tienen valores que van del 192 al 223 en su primer octeto.

Todas las direcciones IP de Clase C utilizan los primeros 24 bits para identificar la porción de red de la dirección. Sólo se puede utilizar el último octeto de una dirección IP de Clase C para la parte de la dirección que corresponde al host. A cada una de las redes que utilizan una dirección IP de Clase C se les pueden asignar hasta 28 (menos 2), o 254, direcciones IP posibles para los dispositivos que están conectados a la red.



Direcciones IP como números decimales

Las direcciones IP identifican un dispositivo en una red, y la red a la cual se encuentra conectado. Para que sea fácil recordarlas, las direcciones IP generalmente están escritas en *notación decimal punteada* (4 números decimales separados por puntos, por ejemplo, 166.122.23.130; tenga en cuenta que un número decimal es un número de base 10, el tipo de número que usamos diariamente).



Propósitos de los identificadores de red y direcciones de broadcast

Si su computador deseara comunicarse con todos los dispositivos de una red, será prácticamente imposible escribir la dirección IP para cada dispositivo. Se puede hacer el intento con dos direcciones separadas por guiones, que indica que se está haciendo referencia a todos los dispositivos dentro de un intervalo de números, pero esto también será excesivamente complicado. Existe, sin embargo, un método abreviado.

Una dirección IP que termina en 0 binarios en todos los bits de host se reserva para la dirección de red (a veces denominada la *dirección* de cable). Por lo tanto, como ejemplo de una red de Clase A, 113.0.0.0 es la dirección IP de la red que contiene el host 113.1.2.3. Un router usa la dirección IP de una red al enviar datos en Internet. Como ejemplo de una red de Clase B, la dirección IP 176.10.0.0 es una dirección de red.

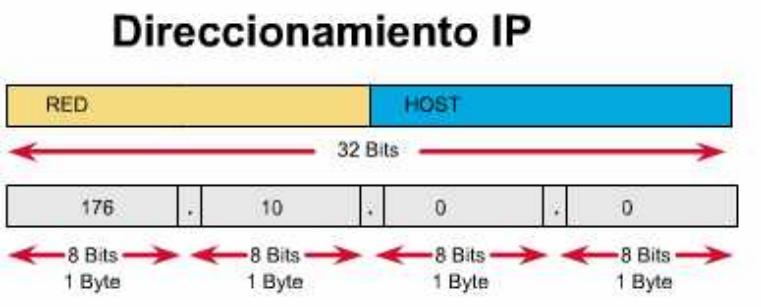
Los números decimales que completan los dos primeros octetos de una dirección de red Clase B se asignan y son números de red. Los últimos dos octetos tienen 0, dado que esos 16 bits corresponden a los números de host y se utilizan para los dispositivos que están conectados a la red. La dirección IP en el ejemplo (176.10.0.0) se encuentra reservada para la dirección de red. Nunca se usará como dirección para un dispositivo conectado a ella.

Si desea enviar datos a todos los dispositivos de la red, necesita crear una dirección de broadcast. Un broadcast se produce cuando un origen envía datos a todos los dispositivos de una red. Para garantizar que todos los dispositivos en una red presten atención a este broadcast, el origen debe utilizar una dirección IP destino que todos ellos puedan reconocer y captar. Las direcciones IP de broadcast terminan con unos binarios en toda la parte de la dirección que corresponde al host (el *campo de host*).

Para la red del ejemplo (176.10.0.0), donde los últimos 16 bits forman el campo de host (o la parte de la dirección que corresponde al host), el broadcast que se debe enviar a todos los dispositivos de esa red incluye una dirección destino 176.10.255.255 (ya que 255 es el valor decimal de un octeto que contiene 11111111).

ID de red

Es importante entender el significado de la parte de la red IP que corresponde a la red: el *ID de red*. Los hosts de una red sólo se pueden comunicar directamente con los dispositivos que tienen el mismo ID de red. Pueden compartir el mismo segmento físico, pero si tienen distintos números de red, generalmente no pueden comunicarse entre sí, a menos que haya otro dispositivo que pueda realizar una conexión entre las redes.



Analogía de ID de red

Los códigos postales y los ID de red son muy similares en su funcionamiento. Los códigos postales permiten que el servicio postal pueda enviar el correo a su oficina postal local y a su vecindad. A partir de allí, la dirección de la calle indica al cartero el destino correcto. Un ID de red habilita el router a colocar el paquete en el segmento de red apropiado, mientras que el ID de host ayuda al router a direccionar la trama de Capa 2 (encapsulando el paquete) hacia el host específico en esa red.

Analogía de la dirección de broadcast

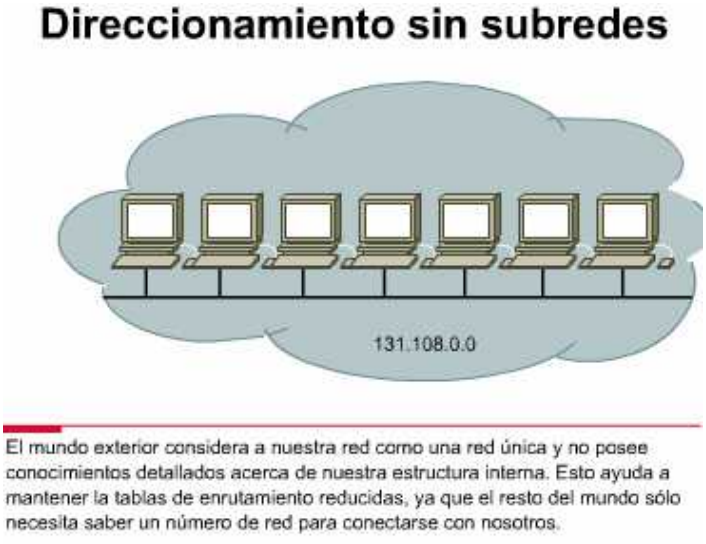
Una dirección de broadcast es una dirección compuesta exclusivamente por números unos en el campo de host. Cuando se envía un paquete de broadcast en una red, todos los dispositivos de la red lo captan. Por ejemplo, en una red con un identificador 176.10.0.0, el mensaje de broadcast que llega a todos los hosts tendría la dirección 176.10.255.255.

Una dirección de broadcast es bastante similar al envío de correo masivo. El código postal dirige el correo hacia el área correspondiente, y la dirección de broadcast "Residente actual" vuelve a dirigir el correo hacia cada una de las direcciones. Una dirección IP de broadcast utiliza el mismo concepto. El número de red designa el segmento y el resto de la dirección le indica a cada host IP de esa red que éste es un mensaje de broadcast y que cada dispositivo debe prestar atención al mensaje. Todos los dispositivos en una red reconocen su propia dirección IP del host, así como la dirección de broadcast de la red.

Direccionamiento IP clásico

Los administradores de redes a veces necesitan dividir las redes, especialmente las de gran tamaño, en redes más pequeñas denominadas subredes, para brindar mayor flexibilidad.

De manera similar a lo que ocurre con la porción del número de host de las direcciones de Clase A, Clase B y Clase C, las direcciones de subred son asignadas localmente, normalmente por el administrador de la red. Además, tal como ocurre con otras direcciones IP, cada dirección de subred es única



Subred

Las direcciones de subred incluyen la porción de red de Clase A, Clase B o Clase C además de un campo de subred y un campo de host. El campo de subred y el campo de host se crean a partir de la porción de host original para toda la red. La capacidad de decidir cómo dividir la porción de host original en los nuevos campos de subred y de host ofrece flexibilidad para el direccionamiento al administrador de red. Para crear una dirección de subred, un administrador de red pide prestados bits de la parte original de host y los designa como campo de subred.

Para crear una dirección de subred, un administrador de red pide prestados bits del campo de host y los designa como campo de subred. La cantidad mínima de bits que se puede pedir prestada es 2. Si fuera a pedir prestado sólo 1 bit para crear una subred, entonces sólo tendría un número de red (el.0 de red) y el número de broadcast (el .1 de red). La cantidad mínima de bits que se puede pedir prestada puede ser cualquier número que deje por lo menos 2 bits restantes para el número de host. En este ejemplo de una Dirección IP de Clase C, se han pedido prestados bits del campo de host para el campo de subred.

Propósito de la división en subredes

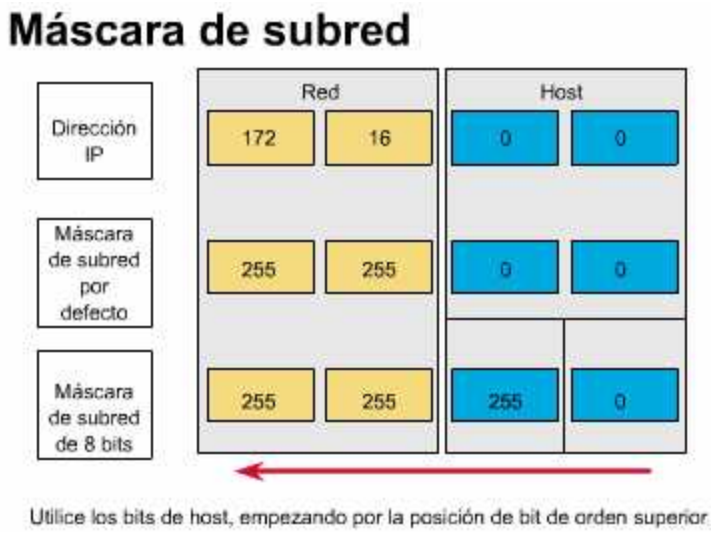
La razón principal para usar una subred es reducir el tamaño de un dominio de broadcast. Se envían broadcasts a todos los hosts de una red o subred. Cuando el tráfico de broadcast empieza a consumir una porción demasiado grande del ancho de banda disponible, los administradores de red pueden preferir reducir el tamaño del dominio de broadcast.

Máscara de subred

La máscara de subred (término formal: prefijo de red extendida), le indica a los dispositivos de red cuál es la parte de una dirección que corresponde al campo de red y cuál es la parte que corresponde al campo de host. Una máscara de subred tiene una longitud de 32 bits y tiene 4 octetos, al igual que la dirección IP.

Para determinar la máscara de subred para una dirección IP de subred particular, siga estos pasos. (1) Exprese la dirección IP de subred en forma binaria. (2) Cambie la porción de red y subred de la dirección por todos unos. (3) Cambie la porción del host de la dirección por todos ceros. (4) Como último paso, convierta la expresión en números binarios nuevamente a la notación decimal punteada.

Nota: El prefijo de red extendida incluye el número de red de clase A, B o C y el campo de subred (o número de subred) que se utiliza para ampliar la información de enrutamiento (que de otro modo es simplemente el número de red).



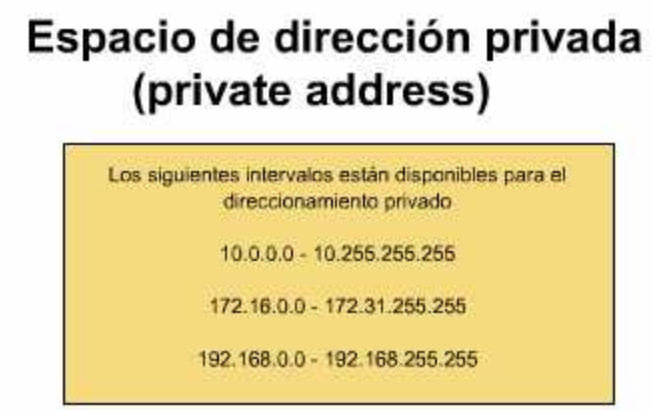
Direcciones privadas

Hay ciertas direcciones en cada clase de dirección IP que no están asignadas. Estas direcciones se denominan direcciones privadas. Las direcciones privadas pueden ser utilizadas por los hosts que usan *traducción de dirección de red* (*NAT*), o un *servidor proxy* , para conectarse a una red pública o por los hosts que no se conectan a Internet.

Muchas aplicaciones requieren conectividad dentro de una sola red, y no necesitan conectividad externa. En las redes de gran tamaño, a menudo se usa TCP/IP, aunque la conectividad de capa de red no sea necesaria fuera de la red. Los bancos son buenos ejemplos. Pueden utilizar TCP/IP para conectar los cajeros automáticos (ATM). Estas máquinas no se conectan a la red pública, de manera que las direcciones privadas son ideales para ellas. Las direcciones privadas también se pueden utilizar en una red en la que no hay suficientes direcciones públicas disponibles.

Las direcciones privadas se pueden utilizar junto con un servidor de traducción de direcciones de red (NAT) o servidor proxy para suministrar conectividad a todos los hosts de una red que tiene relativamente pocas direcciones públicas disponibles. Según lo acordado, cualquier tráfico que posea una dirección destino dentro de uno de los intervalos de direcciones privadas NO se enrutará a través de Internet.

Los siguientes intervalos de direcciones están disponibles para el direccionamiento privado :



Métodos para asignar una dirección IP

Una vez que ha determinado el esquema de direccionamiento para una red, debe seleccionar el método para asignar direcciones a los hosts. Existen principalmente dos métodos de asignación de direcciones IP: el direccionamiento estático y el direccionamiento dinámico.

Independientemente de qué esquema de direccionamiento utilice, dos interfaces no pueden tener la misma dirección IP.

Direccionamiento estático

Si asigna direcciones IP de modo estático, debe ir a cada dispositivo individual y configurarlo con una dirección IP. Este método requiere que se guarden registros muy detallados, ya que pueden ocurrir problemas en la red si se utilizan direcciones IP duplicadas. Algunos sistemas operativos como, por ejemplo, Windows 95 y Windows NT, envían una petición ARP para verificar si existe una dirección IP duplicada cuando tratan de inicializar TCP/IP. Si descubren que hay una dirección duplicada, los sistemas operativos no inicializan TCP/IP y generan un mensaje de error. Además, es importante mantener registros porque no todos los sistemas operativos identifican las direcciones IP duplicadas.

Direccionamiento dinámico

Hay varios métodos distintos que se pueden usar para asignar direcciones IP de forma dinámica. Ejemplos de estos métodos son:

Protocolo de resolución de dirección inversa (RARP)

El Protocolo de resolución de dirección inversa (RARP) relaciona las direcciones MAC con las direcciones IP. Esta relación permite que algunos dispositivos de la red encapsulen los datos antes de enviarlos a través de la red. Es posible que un dispositivo de red, como, por ejemplo, una estación de trabajo sin disco conozca su dirección MAC pero no su dirección IP. Los dispositivos que usan RARP requieren que haya un servidor RARP en la red para responder a las peticiones RARP.

Veamos un ejemplo donde un dispositivo origen desea enviar datos a otro dispositivo y que el origen conoce su dirección MAC pero no puede ubicar su dirección IP en la tabla ARP. Para que el dispositivo destino pueda recuperar los datos, los pase a capas superiores del modelo OSI y responda al dispositivo origen, el origen debe incluir tanto la dirección MAC como la dirección IP. Por lo tanto, el origen inicia un proceso denominado petición RARP, que lo ayuda a detectar su propia dirección IP. El dispositivo crea un paquete de petición RARP y lo envía a través de la red. Para asegurarse de que todos los dispositivos de la red vean la petición RARP, usa una dirección de broadcast IP.

Una petición RARP está compuesta por un encabezado MAC, un encabezado IP y un mensaje de petición ARP. El formato del paquete RARP contiene lugares para las direcciones MAC tanto destino como origen. El campo de la dirección IP origen está vacío. El broadcast se transmite a todos los dispositivos de la red; en consecuencia, la dirección IP destino se establece con números unos binarios exclusivamente. Las estaciones de trabajo que ejecutan RARP tienen códigos en la ROM que les hacen iniciar el proceso RARP y ubicar el servidor RARP.

Protocolo BOOTstrap (BOOTP)

Un dispositivo usa el protocolo BOOTstrap (BOOTP) cuando se inicia, para obtener una dirección IP. BOOTP usa el Protocolo de datagrama de usuario (UDP) para transportar mensajes; el mensaje UDP se encapsula en un datagrama IP. Un computador utiliza BOOTP para enviar un datagrama IP de broadcast (usando una dirección IP destino de todos unos: 255.255.255.255). Un servidor BOOTP recibe el broadcast y luego envía un broadcast. El cliente recibe un datagrama y verifica la dirección MAC. Si encuentra su propia dirección MAC en el campo de dirección destino, entonces acepta la dirección IP del datagrama. Como en el caso de RARP, BOOTP opera en un entorno de cliente-servidor y sólo requiere un intercambio de paquetes. Sin embargo, a diferencia de RARP, que solamente envía de regreso una dirección IP de 4 octetos, los datagramas BOOTP pueden incluir la dirección IP, la dirección de un router (gateway por defecto), la dirección de un servidor y un campo específico para el fabricante. Uno de los problemas de BOOTP es que no fue diseñado para suministrar una asignación de direcciones dinámica. Con BOOTP usted puede crear un archivo de configuración que especifique los parámetros para cada dispositivo.

Protocolo de configuración dinámica del host (DHCP)

El Protocolo de configuración dinámica del host (DHCP) se ha propuesto como sucesor del BOOTP. A diferencia del BOOTP, DHCP permite que un host obtenga una dirección IP de forma rápida y dinámica. Todo lo que se necesita al usar el servidor DHCP es una cantidad definida de direcciones IP en un servidor DHCP. A medida que los hosts entran en línea, se ponen en contacto con el servidor DHCP y solicitan una dirección. El servidor DHCP elige una dirección y se asigna a ese host. Con DHCP, se puede obtener la configuración completa del computador en un solo mensaje (por Ej., junto con la dirección IP, el servidor también puede enviar una máscara de subred).

Componentes IP claves

Para que los dispositivos se puedan comunicar, los dispositivos emisores necesitan tanto las direcciones IP como las direcciones MAC de los dispositivos destino. Cuando tratan de comunicarse con dispositivos cuyas direcciones IP conocen, deben determinar las direcciones MAC. El conjunto TCP/IP tiene un protocolo, denominado ARP, que puede detectar automáticamente la dirección MAC. ARP permite que un computador descubra la dirección MAC del computador que está asociado con una dirección IP.
Nota: La unidad básica de transferencia de datos en IP es el *paquete IP* . El procesamiento de datagramas se lleva a cabo en el software, lo que significa que el contenido y el formato no dependen del hardware. El datagrama se divide en dos componentes principales: el encabezado, que incluye las direcciones origen y destino, y los datos. Otros tipos de protocolos tienen sus propios formatos. El datagrama IP es exclusivo de IP.

Apéndice 2

Tutorial de IPV6

Tutorial de IPV6

Los motivos de IPv6

El motivo básico por el que surge, en el seno del IETF (Internet Engineering Task Force), la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generation, o "Siguiente Generación d Protocolo Internet"), fue la evidencia de la falta de direcciones.
IPv4 tiene un espacio de direcciones de 32 bits, es decir, 2^{32} (4.294.967.296).

En cambio, IPv6 nos ofrece un espacio de 2^{128}
(340.282.366.920.938.463.463.374.607.431.768.211.456).

Sin embargo, IPv4 tiene otros problemas o "dificultades" que IPv6 soluciona o mejora.
Los creadores de IPv4, a principio de los años 70, no predijeron en ningún momento, el gran éxito que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

Podemos recordar algunas "famosas frases" que nos ayudarán a entender hasta que punto, los propios 'precursores' de la revolución tecnológica que estamos viviendo, no llegaron a prever:

"Pienso que el mercado m undial de ordenadores puede ser de cinco unidades", Thomas Watson, Presidente de IBM en 1.943

"640 Kbps. de memoria han de ser suficientes para cualquier usuario", Bill Gates, Presidente de Microsoft, 1.981

"32 bits proporcionan un espacio de direccionam iento suficiente para Internet", Dr. Vinton Cerf, padre de Internet, 1.977

No es que estuvieran equivocados, sino que las Tecnologías de la Información han evolucionado de un modo mucho más explosivo de lo esperado. Además, ¿no dice el dicho "es de sabios rectificar"?
Desde ese momento, y debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico.

Entre los "parches" más conocidos, podemos citar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec), y Movilidad, fundamentalmente.

El inconveniente más importante de estas ampliaciones de IPv4, es que utilizar cualquiera de ellos es muy fácil, pero no tanto cuando pretendemos usar al muy poco práctico el uso simultáneo de tres o más, llegando a ser un auténtico malabarismo de circo.

¿Porqué IPv6?

La ventaja fundamental de IPv6 es el espacio de direcciones.
El reducido espacio de IPv4, a pesar de disponer de cuatro mil millones de direcciones (4.294.967.296), junto al hecho de una importante falta de coordinación, durante la década de los 80, en la delegación de direcciones, sin ningún tipo de optimización, dejando incluso grandes espacios discontinuos, nos esta llevando a límites no sospechados en aquel momento.
Por supuesto, hay una solución que podríamos considerar como evidente, como sería la renumeración, y reasignación de dicho espacio de direccionamiento.
Sin embargo, no es tan sencillo, es incluso impensable en algunas redes, ya que requiere unos esfuerzos de coordinación, a escala mundial, absolutamente impensables.
Además, uno de los problemas de IPv4 permanecería: la gran dimensión de las tablas de enrutado (routing) en el troncal de Internet, que la hace ineficaz, y perjudica enormemente los tiempos de respuesta.
La falta de direcciones no es apreciable por igual en todos los puntos de la red, de hecho, no es casi apreciable, por el momento, en Norte América. Sin embargo, en zonas geográficas como Asia (en Japón la situación esta llegando a ser crítica), y Europa, el problema se agrava.
Como ejemplos, podemos citar el caso de China que ha pedido direcciones para conectar 60.000 escuelas, tan sólo ha obtenido una clase B (65.535 direcciones), o el de muchos países Europeos, Asiáticos y Africanos, que solo tienen una clase C (255 direcciones) para todo el país.
Tanto en Japón como en Europa el problema es creciente, dado al importante desarrollo de las redes de telefonía celular, inalámbricas, módems de cable, xDSL, etc., que requieren direcciones IP fijas para aprovechar al máximo sus posibilidades e incrementar el número de aplicaciones en las que pueden ser empleados.
La razón de utilización de las direcciones IP por parte de los usuarios, esta pasando en pocos meses de 10:1 a 1:1, y la tendencia se invertirá. En pocos meses, podemos ver dispositivos "siempre conectados", con lo que fácilmente un usuario podría tener, en un futuro no muy lejano, hasta 50 o 100 IP's (1:50 o 1:100).
Algunos Proveedores de Servicios Internet se ven incluso obligados a proporcionar a sus clientes direcciones IP privadas, mediante mecanismos de NAT (traslación de direcciones, es decir, usar una sola IP pública para toda una red privada). De hecho, casi todos los PSI's se ven obligados a delegar tan sólo reducidos números de direcciones IP públicas para sus grandes clientes corporativos.

Como ya se ha dicho, la solución, temporalmente, es el uso de mecanismos NAT. Desafortunadamente, de seguir con IPv4, esta tendencia no sería "temporal", sino "invariablemente permanente". Ello implica la imposibilidad práctica de muchas aplicaciones, que quedan relegadas a su uso en Intranets, dado que muchos protocolos son incapaces de atravesar los dispositivos NAT:

RTP y RTCP ("Real-time Transport Protocol" y "Real Time Control Protocol") usan UDP con asignación dinámica de puertos (NAT no soporta esta traslación).
La autenticación Kerberos necesita 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 tan complicada
con NAT, que en la práctica no se emplea.

Cifras actuales y proyecciones del crecimiento de Internet

Las cifras de "internautas", esperadas en los próximos años, avalan lo expuesto:

- Africa: 800.000.000 (sólo 3.000.000 sin NAT)
- América Central y del Sur: 500.000.000 (sólo 10.000.000 sin NAT)
- América del Norte: 500.000.000 (sólo 125.000.000 sin NAT)
- Asia: 2.500.000.000 (sólo 50.000.000 sin NAT)
- Europa Occidental: 250.000.000 (sólo 50.000.000 sin NAT)

Pero lo más importante es el imparable crecimiento de aplicaciones que necesitan direcciones IP públicas únicas, globales, válidas para conexiones extremo a extremo, y por tanto encaminables (enrutables): Videoconferencia, Voz sobre IP, seguridad, e incluso juegos.

Veamos más cifras. Sólo en Estados Unidos de América, el mercado potencial de aplicaciones susceptibles de ser conectadas a la red, según Driscol & Associates, en un estudio del año 1.995, era:

MERCADO VERTICAL	EJEMPLOS DE APLICACIÓN	TAMAÑO DEL MERCADO
Lectura de Contadores	Lectura de consumos de agua, gas, electricidad, etc.	242.000.000
Seguridad	Sistemas de alarma, incendios, etc., tanto residenciales como comerciales	24.000.000
Posicionamiento de Vehículos/flotas e información de condiciones	Seguimiento automático de vehículos Seguimiento de inventarios Diagnóstico y seguridad de vehículos	15.000.000
Monitorización	Máquinas de venta automática (vending) Buzones de correo Gas e irrigación	7.900.000
	Total	**288.900.000**

En 1.997, el mercado de dispositivos con aplicaciones capaces de conectarse a Internet (sin incluir terminales ni ordenadores, tan sólo WebTV, agendas electrónicas, teléfonos con acceso a Internet, y consolas de juegos), era de 3.000.000. En el año 1.998, este se duplica hasta llegar a los 6.000.000, y las previsiones de crecimiento para el 2.002, según IDC, son de 56.000.000. Sólo contabilizando el crecimiento de la nueva generación de telefonía móvil

(UMTS), en el año 2.003 se sobrepasan las cifras del orden de los 1.000.000.000 de usuarios, la misma cifra que para la telefonía fija y que para el número de usuarios "fijos" de Internet. En ese momento, los usuarios móviles con conexión a Internet superan a los 400.000.000.

El mismo Foro UMTS/GSM prevé unas necesidades de direcciones IP para los dispositivos de la red (no para los dispositivos de los usuarios), para el año 2.005, de 3,2 millones, y de 6,3 para el 2.010. Según el mismo informe, en el 2.005, se requerirían un total de 20.000.000.000 de direcciones IP para los dispositivos de los usuarios.

A esto hemos de sumar los innumerables dispositivos que vamos creando, o los ya existentes a los que damos nuevas o mejoradas aplicaciones, mediante su conexión a la red, valgan como ejemplos:
Teléfonos, pues la siguiente generación, sin duda, pasara por tecnologías IP (VoIP).
Televisión y Radio, también basados en tecnologías IP.
Sistemas de seguridad, televigilancia y control.
Frigoríficos que evalúan nuestros hábitos de consumo y nos dan la opción de

a) imprimir la lista de la compra,
b) hacer el pedido en el supermercadopara que nos sea entregado automáticamente,
c) hacer el pedido para que pasemos a recogerlo decidiendo "in situ" el resto de la compra,
d) navegar por un superercado virtual y permitirnos llenar el carro según nuestros hábitos añadiendo nuestros caprichos ocasionales.
e) Despertadores, que conocen nuestros tiempos de desplazamiento habituales a nuestro lugar de trabajo, y con motivo de un accidente o gran nevada, de los que son informados mediante los servicios de la red, calculan el tiempo adicional que necesitamos y nos levantan con la anticipación precisa, ¡aún a riesgo de que los destrocemos al arrojarlos contra la pared!
f) Walkman MP3, que conectados a la red, nos permiten recuperar y almacenar creaciones musicales.
g) Nuevas tecnología emergentes, como Bluetooth, WAP, redes inalámbricas, redes domésticas, etc., hacen más patente esta necesidad de crecimiento, al menos, en los que al número de direcciones se refiere. Por ejemplo, la última tendencia es la de permitir a cualquier dispositivo serie, ser conectado a una LAN o WAN, y por que no a Internet. Este tipo de "convertidores", denominados "Universal Device Server", o Servidor de Dispositivos Universal, permite que aplicaciones impensables por las limitaciones de los cableados serie, se realicen remotamente a través de redes, o incluso que un sistema de alarmas, que antes requería un módem dedicado para la conexión con la central de recepción de alarmas, pueda ahora enviar un e-mail, ¡ con todo lujo de detalles !.

Podríamos hablar, en general, de casi cualquier dispositivo tanto doméstico como industrial, integrado en la gran red, pero también en dispositivos de control médico, marcapasos, etc.

Características principales de IPv6

Si resumimos las características fundamentales de IPv6 obtenemos la siguiente relación:

! Mayor espacio de direcciones.

! "Plug & Play": Autoconfiguración.

! Seguridad intrínseca en el núcleo del protocolo (IPsec).

! Calidad de Servicio (QoS) y Clase de Servicio (CoS).

! Multicast: Envío de UN mismo paquete a un grupo de receptores.

! Anycast: Envío de UN paquete a UN receptor dentro de UN grupo.

! Paquetes IP eficientes y extensibles, sin que haya fragmentación en los enrutadores (routers), alineados a 64 bits (preparados para su procesado óptimo con los nuevos procesadores de 64 bits), y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del enrutador (router).

! Posibilidad de paquetes con carga útil (datos) de más de 65.535 bytes.

! Enrutado (enrutado) más eficiente en el troncal (backbone) de la red, debido a una jerarquía de direccionamiento basada en la agregación.

! Renumeración y "multi-homing", que facilita el cambio de proveedor de servicios.

! Características de movilidad.

Pero hay que insistir, de nuevo, en que estas son las características básicas, y que la propia estructura del protocolo permite que este crezca, o dicho de otro modo, sea escalado, según las nuevas necesidades y aplicaciones o servicios lo vayan precisando. Precisamente, la escalabilidad es la baza más importante de IPv6 frente a I P v 4 .

Los cimientos de IPv6

Los criterios que se han seguido a lo largo del desarrollo de IPv6 han sido fundamentales para obtener un protocolo sencillo y al mismo tiempo extremadamente consistente y escalable.
Son de destacar, entre estos criterios, además de todo lo dicho hasta el momento (número de direcciones, seguridad, movilidad y autoconfiguración) la especial aptitud para ser soportado por plataformas existentes, y una evolución que permite su uso concurrente con IPv4: No es necesario realizar un cambio "instantáneo en una fecha X", sino que el cambio es transparente.

Estos criterios se han alcanzado en gran medida por la ortogonalidad y simplificación de la cabecera de longitud fija, lo que redunda en la eficacia de su enrutado (enrutado), tanto en pequeños enrutadores como en los más grandes, con soportes de ancho de banda muy superiores a los 100 Gbytes con
los dispositivos actuales.
Los equipos actuales, a pesar de sus tremendas capacidades de procesamiento de paquetes, no serían capaces de acometer la misma tarea, ni de ofrecer soluciones a todas las necesidades emergentes, con la estructura de la cabecera IPv4, sin contar la imposibilidad de gestionar las tablas de enrutado de los troncales, si siguen creciendo al ritmo actual.

Especificaciones básicas de IPv6 (RFC2460)

Veamos, en primer lugar, la descripción de la cabecera de un paquete IPv4:

Como vemos, la longitud mínima de la cabecera IPv4 es de 20 bytes (cada fila de la tabla supone 4 bytes). A ello hay que añadir las opciones, que dependen de cada caso. En la tabla anterior hemos usado abreviaturas, en aquellos casos en los que son comunes. En el resto, nuestra "particular" traducción de la nomenclatura original anglosajona, cuya "leyenda de equivalencias" indicamos a continuación:

V e r s i o n – Versión (4 bits)
H e a d e r – Cabecera (4 bits)
TOS (Type Of Service) – Tipo de Servicio (1 byte)
Total Length – Longitud Total (2 bytes)
I d e n t i f i c a t i o n – Identificación (2 bytes)
F l a g – Indicador (4 bits)
Fragment Offset – Desplazamiento de Fragmentación (12 bits – 1.5 bytes)
TTL (Time To Live) – Tiempo de Vida (1 byte)
P r o t o c o l – Protocolo (1 byte)
C h e c k s u m – Código de Verificación (2 bytes)
32 bit Source Address – Dirección Fuente de 32 bits (4 bytes)
32 bit Destination Address – Dirección Destino de 32 bits (4 byt e s)

En la tabla anterior, hemos marcado, mediante el color rojo, los campos que van a desaparecer en IPv6, y los que son modificados, según el siguiente esquema:

Hemos pasado de tener 12 campos, en IPv4, a tan solo 8 en IPv6.
El motivo fundamental por el que los campos son eliminados, es la innecesaria redundancia. En IPv4 estamos facilitando la misma información de varias formas. Un caso muy 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, etc.).

El caso del campo de "Desplazamiento de Fragmentación", es ligeramente diferente, dado que el mecanismo por el que se realiza la fragmentación de los paquetes es totalmente modificado en IPv6, lo que implica la total "inutilidad" de este campo. En IPv6 los enrutadores no fragmentan los paquetes, sino que de ser precisa, dicha fragmentación/desfragmentación se produce extremo a extremo .

Algunos de los campos son renombrados:

Longitud total longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes.
Protocolo siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los enrutadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).
Tiempo de vida límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1 byte).

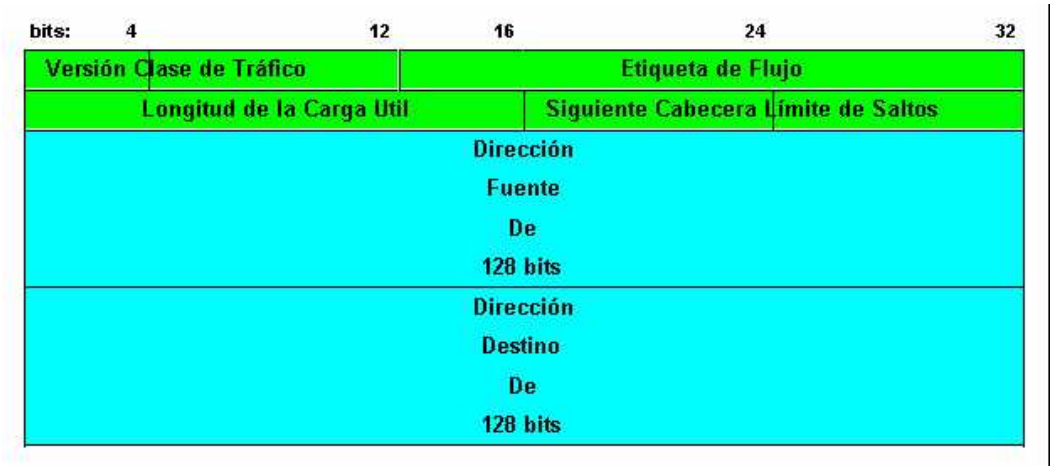
Los nuevos campos son:

Clase de Tráfico (Traffic Class), también denominado Prioridad (Priority), o simplemente Clase (Class). Podría ser más o menos equivalente a TOS en IPv4. Tiene una longitud de 8 bits (1 byte).

Etiqueta de Flujo (Flow Label), para permitir tráficos con requisitos de tiempo real. Tiene una longitud de 20 bits.

Estos dos campos, como se puede suponer, son los que nos permiten una de las características fundamentales e intrínsecas de IPv6: Calidad de Servicio (QoS), Clase de Servicio (CoS), y en definitiva un poderoso mecanismo de control de flujo, de asignación de prioridades diferenciadas según los tipos de servicios.

Por tanto, en el caso de un paquete IPv6, la cabecera tendría el siguiente formato:

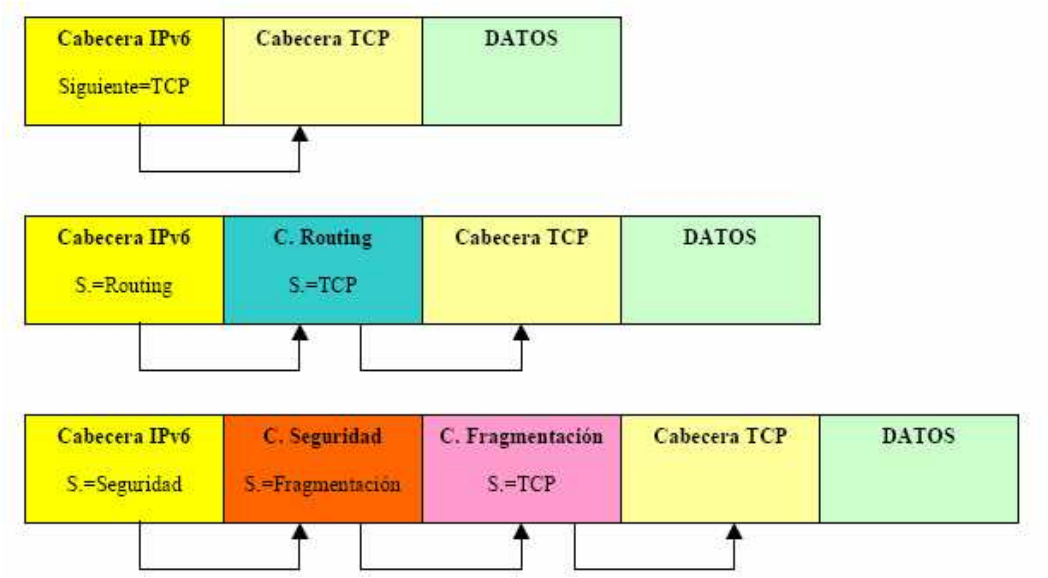


El campo de versión, que es igual a 6, lógicamente, tiene una longitud de 4 bits.La longitud de esta cabecera es de 40 bytes, el doble que en el caso de IPv4, pero con muchas ventajas, al haberse eliminado campos redundantes.

Además, como ya hemos mencionado, la longitud fija de la cabecera, implica una mayor facilidad para su procesado en routers y conmutadores, incluso mediante hardware, lo que implica unas mayores prestaciones. A este fin coadyuva, como hemos indicado anteriormente, el hecho de que los campos están alineados a 64 bits, lo que permite que las nuevas generaciones de procesadores y microcontroladores, de 64 bits, puedan procesar mucho más eficazmente la cabecera IPv6.

El valor del campo "siguiente cabecera", indica cual es la siguiente cabecera y así sucesivamente. Las sucesivas cabeceras, no son examinadas en cada nodo de la ruta, sino sólo en el nodo o nodos destino finales. Hay una única excepción a esta regla: cuando el valor de este campo es cero, lo que indica opción de examinado y proceso "salto a salto" (hop-by-hop). Así tenemos, por citar algunos ejemplos, cabeceras con información de enrutado, fragmentación, opciones de destino, autenticación, encriptación, etc., que en cualquier caso, han de ser procesadas en el orden riguroso en que aparecen en el paquete.

Sin entrar en más detalles, a continuación los siguientes ejemplos gráficos 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):



El MTU (Unidad Máxima de Transmisión), debe de ser como mínimo, de 1.280 bytes, aunque se recomiendan tamaños superiores a 1.500 bytes. Los nodos descubren el valor MTU a través de la inspección de la ruta. Se prevé así una optimización de los paquetes y del número de cabeceras, dado el continuo recimiento de los anchos de banda disponibles, así como del incremento del propio tráfico.
Dado que IPv6 no realiza verificación de errores de la cabecera, en tráfico UDP, se requiere el empleo del su propio mecanismo de checksum.

Direcciones y direccionamiento en IPv6 (RFC2373)

Ya hemos dicho que IPv6 nos aporta, como principio fundamental, un espacio de 2^{128} direcciones, lo que equivale a 3,40E38 (340.282.366.920.938.463.463.374.607.431.768.211.456).

Hagamos una cuenta "rápida", para hacernos a la idea de lo que esta cifra "impronunciable" implica. Calculemos el número de direcciones IP que podríamos tener por metro cuadrado de la superficie terrestre: ¡nada más y nada menos que 665.570.793.348.866.943.898.599!

Indudablemente, hay cabida para todos los dispositivos que podamos imaginar, no solo terrestres, sino interplanetarios. Aunque, por el momento, no podemos asegurar que tenga capacidad para los dispositivos "intergalácticos".

Definición de dirección e n "IPv6"

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

Unicast : Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.

Anycast : Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de enrutado). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing), si la primera "cae".

M u l t i c a s t : Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección. La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).

Diferencias con IPv4

Hay algunas diferencias importantes en el direccionamiento de IPv6 respecto de IPv4:

No hay direcciones broadcast (su función es sustituida por direcciones mult i c a s t) .

Los campos de las direcciones reciben nombres específicos; denominamos "prefijo" a la parte de la dirección hasta el nombre indicado (incluyéndolo). Dicho prefijo nos permite conocer donde esta conectada una determinada dirección, es decir, su ruta de enrutado.

Cualquier campo puede contener sólo ceros o sólo unos, salvo que explícitamente se indique lo contrario.

Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones unicast de las interfaces del nodo puede ser empleado para referirse a dicho nodo.

Todas las interfaces han de tener, al menos, una dirección unicast link-local (enlace local).

Una única interfaz puede tener también varias direcciones IPv6 de cualquier tipo (unicast, anycast o multicast) o ámbito.

Una misma dirección o conjunto de direcciones unicast pueden ser asignados a múltiples interfaces físicas, siempre que la implementación trate dichas interfaces, desde el punto de vista de internet, como una única, lo que permite balanceo de carga entre múltiples dispositivos.

Al igual que en IPv4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiples prefijos de subred a un mismo enlace.

Reservas de espacio de direccionamiento en IPv6

A diferencia de las asignaciones de espacio de direccionamiento que se hicieron en IPv4, en IPv6, se ha reservado , que no "asignado" , algo más del 15%, tanto para permitir una fácil transición (caso del protocolo IPX), como para mecanismos requeridos por el propio protocolo.

Estos son :

Estado	Prefijo (en binario)	Fracción del Espacio
Reservado	0000 0000	1/256
No Asignado	0000 0001	1/256
Reservado para NSAP	0000 001	1/128
Reservado para IPX	0000 010	1/128
No Asignado	0000 011	1/128
No Asignado	0000 1	1/32
No Asignado	0001	1/16
Direcciones Unicast Globales Agregables	001	1/8
No Asignado	010	1/8
No Asignado	011	1/8
No Asignado	100	1/8
No Asignado	101	1/8
No Asignado	110	1/8
No Asignado	1110	1/16
No Asignado	1111 0	1/32
No Asignado	1111 10	1/64
No Asignado	1111 110	1/128
No Asignado	1111 1110 0	1/512
Direcciones Unicast Locales de Enlace	1111 1110 10	1/1.024
Direcciones Unicast Locales de Sitio	1111 1110 11	1/1.024
Direcciones Multicast	1111 1111	1/256

De esta forma se permite la asignación directa de direcciones de agregación, direcciones locales, y direcciones multicast, con reservas para OSI NSAP e IPX. El 85% restantes queda reservado para uso futuro.
Podemos distinguir las direcciones multicast de las unicast por el valor del octeto de mayor orden de la dirección (FF, o 11111111 en binario, indica multicast). En cambio, en el caso de las anycast, no hay ninguna diferencia, sintácticamente hablando, y por tanto, son tomadas del espacio de direcciones unicast.

Direcciones especiales en IPv6

Se han definido también las direcciones para usos especiales como:

Dirección de auto-retorno o Loopback (::1) – No ha de ser asignada a una interfaz física; se trata de una interfaz "virtual", pues se trata de paquetes que no salen de la máquina que los emite; nos permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de una determinada máquina).

Dirección no especificada (::) – Nunca debe ser asignada a ningún nodo, ya que se emplea para indicar la ausencia de dirección; por ejemplo, cuando se halla en el campo de dirección fuente, indica que se trata de un host que esta iniciándose, antes de que haya aprendido su propia dirección.

Túneles dinámicos/automáticos de IPv6 sobre IPv4 (::<dirección IPv4>) – Se denominan direcciones IPv6 compatibles con IPv4, y permiten la retransmisión de tráfico IPv6 sobre infraestructuras IPv4, de forma transparente.

80 bits	**16 bits**	**32 bits**
0000	**... 0000 0000**	**dirección IPv4**

Representación automática de direcciones IPv4 sobre IPv6 (::FFFF:<dirección IPv4>) – permite que los nodos que sólo soportan IPv4, puedan seguir trabajando en redes IPv6. Se denominan "direcciones IPv6 mapeadas desde IPv4".

80 bits	**16 bits**	**32 bits**
0000 ...	**0000 FFFF**	**Dirección IPv4**

Representació n de las direcciones IPv6

La representación de las direcciones IPv6 sigue el siguiente esquema:

a) 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 preciso escribir los ceros a la izquierda de cada campo. Ejemplos:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:417ª

b) Dado que, por el direccionamiento que se ha definido, podrán existir largas cadenas de bits "cero", se permite la escritura de su abreviación, mediante el uso de "::", que representa múltiples grupos consecutivos de 16 bits "cero". Este símbolo sólo puede aparecer una vez en la dirección IPv6. Ejemplos:

Las direcciones:
1080:0:0:0:8:800:200C:417A (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:417A (una dirección unicast)
FF01::101 (una dirección multicast)
::1 (la irección loopback)
:: (una dirección no especificada)

c) Una forma alternativa y muy conveniente, cuando nos hallemos en un entorno mixto IPv4 e IPv6, es x:x:x:x:x:x:d:d:d:d, donde "x" representa valores hexadecimales de 16 bits (6 porciones de mayor peso), y "d" representa valores decimales de las 4 porciones de 8 bits de menor peso (representación estándar IPv4). Ejemplos:

0:0:0:0:0:0:13.1.68.3
0:0:0:0:0:FFFF:129.144.52.38

Pueden representarse como:
: : 1 3 . 1 . 6 8 . 3
::FFFF:129.144.52.38

La representación de los prefijos IPv6 se realiza del siguiente modo:dirección-IPv6/longitud-del-prefijo donde :

- dirección-IPv6 = una dirección IPv6 en cualquiera de las notaciones válidas
- longitud-del-prefijo = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo Por ejemplo, las representaciones válidas del prefijo de 60 bits 12AB00000000CD3, son:
-

12AB:0000:0000:CD30:0000:0000:0000:0000/60
12AB::CD30:0:0:0:0/60
12AB:0:0:CD30::/60

Por tanto, para escribir una dirección completa, indicando la subred, podríamos
hacerlo como:

12AB:0:0:CD30:123:4567:89AB:CDEF/60

Direcciones unicast locales

Las direcciones unicast, son agregables con máscaras de bits contiguos, similares al caso de IPv4, con CIDR (Class-less Interdomain Routing). Como hemos visto, hay varias formas de asignación de direcciones unicast, y otras pueden ser definidas en el futuro.
Los nodos IPv6 pueden no tener ningún conocimiento o mínimo de la estructura interna de las direcciones IPv6, dependiendo de su misión en la red (por ejemplo, host frente a router). Pero como mínimo, un nodo debe considerar que las direcciones unicast (incluyendo la propia), no tienen estructura.

Direcciones anycast (RFC2526)

Tal y como hemos indicado antes, las direcciones anycast tienen el mismo rango de direcciones que las unicast. Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser explícitamente configurados para que reconozcan que se trata de una dirección anycast.

Existe una dirección anycast, requerida para cada subred, que se denomina "dirección anycast del router de la subred" (subnet-router anycast address). Su sintaxis es equivalente al prefijo que especifica el enlace correspondiente de la dirección unicast, siendo el indicador de interfaz igual a cero:

Direcciones multicast (RFC2375)

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

Direcc iones Requeridas para cualquier nodo

Todos los nodos, en el proceso de identificación, al unirse a la red, deben de reconocer como mínimo, las siguientes direcciones:

Sus direcciones locales de enlace para cada interfaz Las direcciones unicast asignadas La dirección de loopback Las direcciones multicast de todos los nodos Las direcciones multicast solicitadas para cada dirección unicast o anycast asignadas Las direcciones multicast de todos los grupos a los que dicho host pertenecen.Además, en el caso de los routers, tienen que reconocer también:
La dirección anycast del router de la subnet, para las interfaces en las que esta configurado para actuar como router Todas las direcciones anycast con las que el router ha sido configurado Las direcciones multicast de todos los routers Las direcciones multicast de todos los grupos a los que el router pertenece .Además, todos los dispositivos con IPv6, deben de tener, predefinidos, los prefijos siguientes:

Dirección no especificada
Dirección de loopback
Prefijo de multicast (FF)
Prefijos de uso local (local de enlace y local de sitio)
Direcciones multicast predefinidas
Prefijos compatibles IPv4

Se debe de asumir que todas las demás direcciones son unicast a no ser que sean específicamente configuradas (por ejemplo las direcciones anycast).

Formato para la representación en URL's (RFC2732)

Cuando navegamos, continuamente aludimos a URL, en muchas ocasiones sin conocer el significado precios de esta abreviatura.
La especificación original (RFC2396), que data del año 1.988, nos dice que Uniform Resource Locator (Localizador de Recurso Uniforme), es un medio simple y extensible para identificar un recurso a través de su localización en la red. Una vez aclarado esto, y de la misma forma que en ocasiones usamos direcciones en formato IPv4 para escribir un URL, se han descrito unas normas para realizar la representación literal de direcciones IPv6 cuando se usan herramientas de navegación WWW.
El motivo por el que ha sido preciso realizar esta definición es bien simple. Con la anterior especificación no estaba permitido emplear el carácter ":" en una dirección, sino como separador de "puerto". Por tanto, si se desea facilitar operaciones tipo "cortar y pegar" (cut and paste), para trasladar direcciones entre diferentes aplicaciones, de forma rápida, era preciso buscar una solución que evitase la edición manual de las direcciones IPv6.
La solución es bien sencilla: el empleo de los corchetes ("[","]") para encerrar la dirección IPv6, dentro de la estructura habitual del URL.
Veamos algunos ejemplos; las direcciones siguientes:

FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
1080:0:0:0:8:800:200C:4171
3ffe:2a00:100:7031::1

1080::8:800:200C:417A
: : 1 9 2 . 9 . 5 . 5
::FFFF:129.144.52.38
2010:836B:4179::836B:4179

Serían representadas como:

http://[FEDC:BA98:7654:3210:FEDC:BA98:7654:3210]:80/index.html
http://[1080:0:0:0:8:800:200C:417A]/index.html
http://[3ffe:2a00:100:7031::1]
http://[1080::8:800:200C:417A]/foo
http://[::192.9.5.5]/ipng
http://[::FFFF:129.144.52.38]:80/index.html
http://[2010:836B:4179::836B:4179]

ICMPv6 (RFC2463)

El Protocolo de Mensajes de Control de Internet (Internet Control MessageProtocol), descrito originalmente en el documento RFC792 para IPv4, ha sido actualizado para permitir su uso bajo IPv6.
El protocolo resultante de dicha modificación es ICMPv6, y se le ha asignado un valor, para el campo de "siguiente cabecera", igual a 58. ICMPv6 es parte integral de IPv6 y debe ser totalmente incorporado a cualquier implementación de nodo IPv6.
ICMPv6 es empleado por IPv6 para reportar errores que se encuentran durante el procesado de los paquetes, así como para la realización de otras funciones relativas a la capa "Internet", como diagnósticos ("ping").

Neighbor Discovery (RFC2461)

En IPv6, el protocolo equivalente, en cierto modo, a ARP en IPv4, es el que denominamos "descubrimiento del vecindario". Sin embargo, incorpora también la funcionalidad de otros protocolos IPv4, como "ICMP Router Discovery" y "ICMP Redirect".
Tal como indica esta "traducción", consiste en el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros, en su mismo enlace, para determinar sus direcciones en la capa de enlace, para localizar los routers, y para mantener la información de conectividad ("reachability") acerca de las rutas a los "vecinos" activos.
El protocolo ND (abreviatura común de "Neighbor Discovery"), también se emplea para mantener limpios los "caches" donde se almacena la información relativa al contexto de la red a la que esta conectado un nodo (host o router), y por tanto para detectar cualquier cambio en la misma.

Cuando un router, o una ruta hacia él, falla, el host buscará alternativas funcionales.
ND emplea los mensajes de ICMPv6, incluso a través de mecanismos de multicast en la capa de enlace, para algunos de sus servicios.
El protocolo ND es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6.
Define, entre otros, mecanismos para: descubrir routers, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios, redirección, balanceo de carga entrante, direcciones anycast, y anunciación de proxies. ND define cinco tipos de paquetes ICMPv6: Solicitud de Router (Router Solicitation) – generado por una interfaz cuando es activada, para pedir a los routers que se "anuncien" inmediatamente.

Tipo en paquete ICMPv6 = 133.
Anunciación de Router (Router Advertisement) – generado por los routers periódicamente (entre cada 4 y 1800 segundos) o como consecuencia de una "solicitud de router", a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempos de vida, configuración de direcciones, límite de salto sugerido, etc. Es fundamental para permitir la renumeración.
Tipo en paquete ICMPv6 = 134.
Solicitud de Vecino (Neighbor Solicitation) – generado por los nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el nodo vecino sigue activo (es alcanzable), así como para detectar las direcciones duplicadas.
Tipo en paquete ICMPv6 = 135.
Anunciación de Vecino (Neighbor Advertisement) – generado por los nodos como respuesta a la "solicitud de vecino", o bien para indicar cambios de direcciones en la capa de enlace.
Tipo en paquete ICMPv6 = 136.
Redirección (Redirect) – generado por los routers para informar a los host de un salto mejor para llegar a un determinado destino. Equivalente, en parte a "ICMP redirect".
Tipo en paquete ICMPv6 = 137.
El protocolo ND, frente a los mecanismos existentes en IPv4, reporta numerosas ventajas:
El descubrimiento de routers es parte de la base del protocolo, no es preciso recurrir a los protocolos de enrutado.
La anunciación de router incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
La anunciación de router incluye los prefijos para el enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la máscara de red.

La anunciación de router permite la autoconfiguración de direcciones Los routers pueden anunciar a los host del mismo enlace el MTU (tamaño máximo de la unidad de transmisión).
Se extienden los multicast de resolución de direcciones entre 2 3 2 direcciones, reduciendo de forma importante las interrupciones relativas a la resolución de direcciones en nodos distintos al objetivo, y evitando las interrupciones en nodos sin IPv6.
Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.

Se pueden asignar múltiples prefijos al mismo enlace y por defecto los host aprenden todos los prefijos por la anunciación de router. Sin embargo, los routers pueden ser configurados para omitir parte o todos los prefijos en la anunciación, de forma que los host consideren que los destinos están fuera del enlace; de esta forma, enviarán el tráfico a los routers, quién a su vez lo redireccionará según corresponda.
A diferencia de IPv4, en IPv6 el receptor de una redirección asume que el siguiente salto esta en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos en el mismo enlace (enlaces sin multidifusión y media compartida).
La detección de vecinos no alcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
A diferencia de ARP, en ND se puede detectar fallos de la mitad del enlace, es decir, con conectividad en un sólo sentido, evitando el tráfico hacia ellos.
A diferencia de IPv4, no son precisos campos de preferencia (para definir la "estabilidad" de los routers). La detección de vecinos no alcanzables sustituirá los caminos desde routers con fallos a otros activos.

El uso de direcciones de enlace local para identificar routers, permite a los hosts que mantengan su asociación con los mismos, en el caso de que se realice una renumeración para usar nuevos prefijos globales.

Al realizar la resolución de direcciones en la capa ICMP, se independiza el protocolo del medio, permitiendo mecanismos de autenticación y seguridad normalizados.
En este RFC (2461) se describe, además, el "modelo conceptual" de las estructuras de datos y su manipulación, que un dispositivo (host o router) requeriría para cumplir los protocolos IPv6. Se trata, pues, de un documento clave para la correcta interpretación de IPv6, cuando se trata de aplicarlo a su uso por parte de desarrolladores.
En resumen, ND reemplaza, con grandes mejoras e importantes ventajas, a ARP.

Autoconfiguración en IPv6 (RFC 2462)

La autoconfiguración es el conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en IPv6. Este mecanismo es el que nos permite afirmar que IPv6 es "Plug & Play".
El proceso incluye la creación de una dirección de enlace local, verificación de que no esta duplicada en dicho enlace y determinación de la información que ha de ser autoconfigurada (direcciones y otra información).
Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6 (stateful o configuración predeterminada), o de forma automática (stateless o descubrimiento automático, sin intervención).
Este protocolo define el proceso de generar una dirección de enlace local, direcciones globales y locales de sitio, mediante el procedimiento automático (stateless).
También define el mecanismo para detectar direcciones duplicadas. La autoconfiguración "stateless" (sin intervención), no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de routers, y no precisa servidores adicionales. Permite a un host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers. Los routers anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras el host genera un "identificador de interfaz", que identifica de forma única la interfaz en la subred. La dirección se compone por la combinación de ambos campos.
En ausencia de router, el host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace. En la autoconfiguración "stateful" (predeterminada), el host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor.
Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host.
Ambos tipos de autoconfiguración (stateless y stateful), se complementan.
Un host puede usar autoconfiguración sin intervención (stateless), para generar su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (stateful).
El mecanismo de autoconfiguración "sin intervención" se emplea cuando no importa la dirección exacta que se asigna a un host, sino tan sólo asegurarse que es única y correctamente enrutable.
El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada host tiene una determinada dirección, asignada manualmente.
Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito). Las direcciones tienen asociado un tiempo de vida, que indican durante cuanto tiempo esta vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de Internet.

Para gestionar la expiración de los vínculos, una dirección pasa a través de dos fases diferentes mientras está asignada a una interfaz. Inicialmente, una dirección es "preferred" (preferida), lo que significa que su uso es arbitrario y no está restringido. Posteriormente, la dirección es "deprecated" (desaprobada), en anticipación a que el vínculo con su interfaz actual va a ser anulado.
Mientras esta en estado "desaprobado", su uso es desaconsejado, aunque no prohibido. Cualquier nueva comunicación (por ejemplo, una nueva conexión TCP), debe usar una dirección "preferida", siempre que sea posible.
Una dirección "desaprobada" debería ser usada tan solo por aquellas aplicaciones que ya la venían utilizando y a las que les es muy difícil cambiar a otra dirección sin interrupción del servicio.
Para asegurarse de que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Este algoritmo es ejecutado para todas las direcciones, independientemente de que hayan sido obtenidas mediante autoconfiguración stateless o stateful.
La autoconfiguración esta diseñada para hosts, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además, los
routers también tienen que "aprobar" el algoritmo de detección de direcciones duplicadas.

Autoconfiguración Stateless

El procedimiento de autoconfiguración stateless (sin intervención o descubrimiento automático), ha sido diseñado con las siguientes premisas:

Evitar la configuración manual de dispositivos antes de su conexión a la red. Se requiere, en consecuencia, un mecanismo que permita a los host obtener o crear direcciones únicas para cada una de sus interfaces, asumiendo que cada interfaz puede proporcionar un identificador único para si misma (identificador de interfaz). En el caso más simple, el identificador de interfaz consiste en la dirección de la capa de enlace, de dicha interfaz. El identificador de interfaz puede ser combinado con un prefijo, para formar la dirección.
Las pequeñas redes o sitios, con máquinas conectadas a un único enlace, no deberían requerir la presencia de un servidor "stateful" o router, como requisito para comunicarse. Para obtener, en este caso, características "plug & play", empleamos las direcciones de enlace local, dado que tienen un prefijo perfectamente conocido que identifica el único enlace compartido, al que se conectan todos los nodos. Cada dispositivo forma su dirección de enlace local anteponiendo el prefijo de enlace local a su identificador de interfaz.
En el caso de redes o sitios grandes, con múltiples subredes y routers, tampoco se requiere la presencia de un servidor de configuración de direcciones "stateful", ya que los host han de determinar, para generar sus

direcciones globales o de enlace local, los prefijos que identifican las subredes a las que se conectan. Los routers generan mensajes periódicos de anunciación, que incluyen opciones como listas de prefijos activos en los enlaces.
La configuración de direcciones debe de facilitar la renumeración de los dispositivos de un sitio, por ejemplo, cuando se desea cambiar de proveedor de servicios. La renumeración se logra al permitir que una misma interfaz pueda tener varias direcciones, que recibe "en préstamo". El tiempo del "préstamo" es el mecanismo por el que se renuevan las direcciones, al expirar los plazos para las viejas, sin que se conceda una prórroga.
Al poder disponer de varias direcciones simultáneamente, permite que la transición no sea "disruptora", permitiendo que ambas, la vieja y la nueva dirección den continuidad a la comunicación durante el período de transición.
Sólo es posible utilizar este mecanismo en enlaces capaces de funciones multicast, y comienza, por tanto, cuando es iniciada o activada una interfaz que permite multicast.
Los administradores de sistemas necesitan la habilidad de especificar que mecanismo (stateless, stateful, o ambos), deben ser usados. Los mensajes de anunciación de los routers incluyen indicadores para esta función.
Los pasos básicos para la autoconfiguración, una vez la interfaz ha sido activada, serían:
a) Se genera la dirección "tentativa" de enlace local, como se ha descrito antes b) Verificar que dicha dirección "tentativa" puede ser asignada (no esta duplicada en el mismo enlace).
c) Si esta duplicada, la autoconfiguración se detiene, y se requiere un procedimiento manual (por ejemplo, usando otro identificador de interfaz).
d) Si no esta duplicada, la conectividad a nivel IP se ha logrado, al asignarse definitivamente dicha dirección "tentativa" a la interfaz en cuestión.
e) Si se trata de un host, se interroga a los posibles routers para indicar al host lo que debe de hacer a continuación.
f) Si no hay routers, se invoca el procedimiento de autoconfiguración "stateful".
g) Si hay routers, estos contestarán indicando fundamentalmente, como obtener las direcciones si se ha de utilizar el mecanismo "stateful", u otra información, como tiempos de vida, etc.

Hay algunos detractores de este mecanismo, ya que implica que cualquier nodo puede ser identificado en una determinada red si se conoce su identificador IEEE (dirección MAC). Por ello, para permitir que la dirección no sea estática, se esta trabajando en el documento draft-ietf-ipngwg-addrconf-privacy-01.txt.

Autoconfiguración Stateful – DHCPv6 (draft -ietf-dhcdhcpv6 - 15.txt)

DHCP para IPv6 es un protocolo UDP cliente/servidor, diseñado para reducir el coste de gestión de nodos IPv6 en entornos donde los administradores precisa

un control sobre la asignación de los recursos de la red, superior al facilitados por el mecanismo de configuración "stateless". Como ya hemos indicado, ambos mecanismos pueden usarse de forma concurrente para reducir el coste de propiedad y administración de la red.
Para lograr este objetivo, se centraliza la gestión de los recursos de la red, tales como direcciones IP, información de enrutado, información de instalación de Sistemas Operativos, información de servicios de directorios, sobre uno o varios servidores DHCP, en lugar de distribuir dicha información en ficheros de configuración locales en cada nodo.
Además, DHCP ha sido diseñado para ser fácilmente extensible con nuevos parámetros de configuración, a través de "extensiones" que incorporan esta nueva información. Al respecto es fundamental el documento dhc-v6exts-12.txt.

Los objetivos de DHCPv6 son:

DHCP es un mecanismo, no una política. La política es establecida por el administrador de la red y DHCP le permite propagar los parámetros adecuados, según dicha política.
DHCP es compatible, lógicamente, con el mecanismo de autoconfiguración "stateless".
DHCP no requiere configuración manual de parámetros de red en clientes DHCP, excepto en casos donde dicha configuración se requiere debido a medidas de seguridad.
DHCP no requiere un servidor en cada enlace, dado que debe funcionar a través de relés DHCP.
DHCP coexiste con nodos configurados estáticamente, así como con implementaciones existentes en la red.
Los clientes DHCP pueden operar en enlaces donde no hay routers IPv6.
Los clientes DHCP proporcionan la habilidad de renumerar la red.
Un cliente DHCP puede hacer múltiples y diferentes peticiones de parámetros de configuración, de uno o varios servidores DHCP simultáneamente.
DHCP proporciona suficiente información para permitir a los servidores DHCP el seguimiento del estado de configuración de los clientes.
DHCP incorpora los mecanismos apropiados de control de tiempo y retransmisiones para operar eficazmente en entornos con una alta latencia y/o reducido ancho de banda.

Los cambios fundamentales entre DHCPv4 y DHCPv6, están basados en el soporte inherente del formato de direccionamiento y autoconfiguación IPv6; son
las siguientes:

La dirección de enlace local permite a un nodo tener una dirección tan pronto como arranca, lo que significa que todos los clientes tienen una dirección IP fuente para localizar un servidor o relé en su mismo enlace.

Los indicadores de compatibilidad BOOTP y broadcast han desaparecido .

El multicast y los ámbitos de direccionamiento permiten el diseño de paquetes de descubrimiento, que definen por si mismos su rango por la dirección multicast, para la función requerida.

La autoconfiguración stateful ha de coexistir e integrarse con la stateless, soportando la detección de direcciones duplicadas y los dos tiempos de vida de IPv6, para facilitar la renumeración automática de direcciones y su gestión.
Se soportan múltiples direcciones por cada interfaz.
Algunas opciones DHCPv4 ya no son precisas, debido a que los parámetros de configuración se obtienen a través de ND o del protocolo de localización de servicios (RFC2165).

De esta forma, se soportan las siguientes funciones nuevas:

Configuración de actualizaciones dinámicas de DNS.
Desaprobación de direcciones, para renumeración dinámica.
Relés preconfigurados con direcciones de servidores, o mediante multicast
Autenticación.
Los clientes pueden pedir múltiples direcciones IP.
Las direcciones pueden ser reclamadas mediante el mensaje de "iniciarreconfiguración".
Integración entre autoconfiguración de direcciones "stateless" y "stateful"

Renumeración

En los párrafos anteriores ya hemos descrito el mecanismo básico de renumeración, basado en el "préstamo" o alquiler de direcciones, en las fases de"preferida" y "desaprobada", y en el tiempo de vida de las mismas.
En cualquier caso, podemos describir el mecanismo de forma sencilla, como consistente en disminuir el tiempo de vida del prefijo en los paquetes de anunciación del router, de forma que las direcciones pasen a ser desaprobadas, frente a las nuevas, que pasan a ser preferidas.
Sin embargo, este mecanismo está básicamente diseñado para los host.
En el caso de los routers, se trabaja en un nuevo documento "draft-ietf-ipngwgrouter-renum-10.txt", que permitirá mecanismos similares y más adecuados.

IPv6 sobre Ethernet (RFC2464)

Aunque ya han sido definidos protocolos para permitir el uso de IPv6 sobre cualquier tipo de red o topología (Token Ring, FDDI, ATM, PPP, ...), como

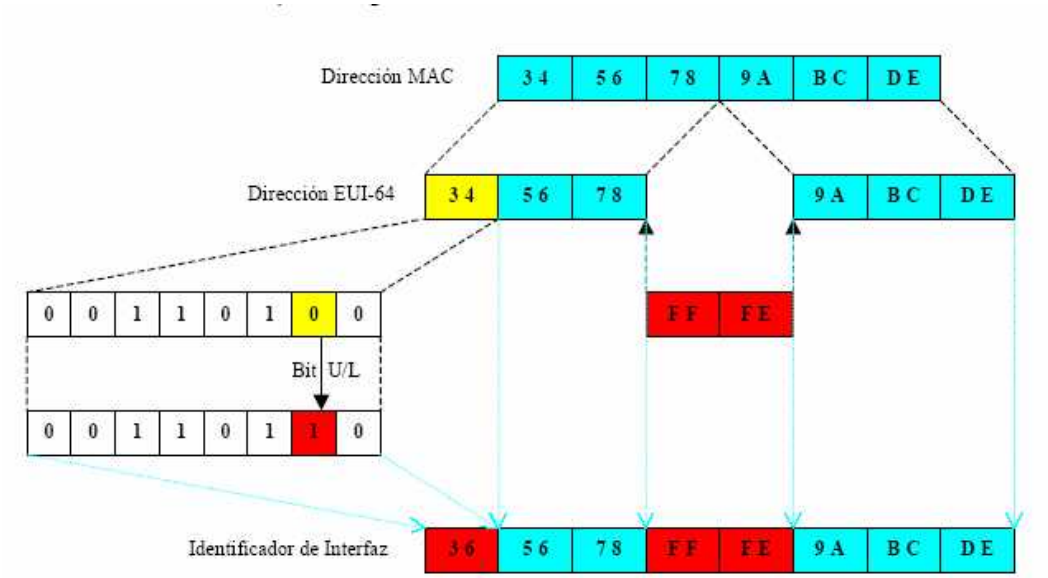
ejemplo mucho más habitual y básico, centraremos este apartado en Ethernet (CSMA/CD y tecnologías full-duplex basadas en ISO/IEC8802-3). Mas adelante, en este mismo documento, citaremos los protocolos adecuados para cada una de las otras tecnologías.
Los paquetes IPv6 se transmiten sobre tramas normalizadas Ethernet. La cabecera Ethernet contiene las direcciones fuente y destino Ethernet, y el código de tipo Ethernet con el valor hexadecimal 86DD.
El campo de datos contiene la cabecera IPv6 seguida por los propios datos, y probablemente algunos bytes para alineación/relleno, de forma que se alcance el tamaño mínimo de trama para el enlace Ethernet.

48 bits	48 bits	16 bits	
Dirección Ethernet Destino	Dirección Ethernet Fuente	1000011011011101 (86DD)	Cabecera y datos IPv6

Cabecera y datos IPv6

El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre Ethernet, es de 1.500 bytes. Evidentemente, este puede ser reducido, manual o automáticamente (por los mensajes de anunciación de routers).
Para obtener el identificador de interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, nos basamos en la dirección MAC de 48 bits (IEEE802). Tomamos los 3 primeros bytes (los de mayor orden), y les agregamos "FFFE" (hexadecimal), y a continuación, el resto de los bytes de la dirección MAC (3 bytes). El identificador así formado se denomina identificador EUI-64 (Identificador Global de 64 bits), según lo define IEEE.
El identificador de interfaz se obtiene, a continuación, partiendo del EUI-64, complementando el bit U/L (Universal/Local). El bit U/L es el siguiente al de menor valor del primer byte del EUI-64 (el 2º bit por la derecha, el 2º bit de menor peso).
Al complementar este bit, por lo general cambiará su valor de 0 a 1; dado que se espera que la dirección MAC sea universalmente única, U/L tendrá un valor 0, y por tanto se convertirá en 1 en el identificador de interfaz IPv6.
Una dirección MAC configurada manualmente o por software, no debería ser usada para derivar de ella el identificador de interfaz, pero si no hubiera otra fórmula, su propiedad debe reflejarse en el valor del bit U/L.

Véase el esquema siguiente:



Para mapear direcciones unicast IPv6 sobre Ethernet, se utilizan los mecanismos ND para solicitud de vecinos.
Para mapear direcciones multicast IPv6 sobre Ethernet, se emplean los 4 últimos bytes de la dirección IPv6, a los que se antepone "3333".

Multi-homing

Como venimos viendo, el mecanismo de asignación de direcciones IPv6 es totalmente jerárquico.
El multi-homing ("múltiples hogares") es el mecanismo por el cual un determinado sitio o red puede estar conectado a otros por múltiples caminos, por razones de seguridad, redundancia, ancho de banda, balanceo de carga, etc.
Dado que un determinado sitio utiliza el prefijo de su ISP, o proveedor de nivel superior, un sitio puede ser "multi-homed" simplemente teniendo varios prefijos.
Frecuentemente, cada prefijo estará asociado a diferentes conexiones físicas, aunque no necesariamente, dado que se puede tratar de una sola conexión física y diversos túneles o conexiones virtuales.

IPsec

Una de las grandes ventajas de IPv6 es, sin duda, la total integración de los mecanismos de seguridad, autenticación y confidencialidad (encriptación), dentro del núcleo del protocolo.
Se trata por tanto de algo obligatorio, y no adicional ni "añadido" como en IPv4. Para ello, la siguiente cabecera puede tener valores AH (autenticación – "Authentication Header") y ESP (encriptación – "Encapsulation Security Payload"), que permiten, básicamente, emplear las mismas extensiones de

protocolo empleadas en IPv4, y que de hecho, al haber sido desarrolladas con posterioridad al inicio de los trabajos de IPv6, ya lo contemplan.
Para mas información al respecto se puende encontrar en: RFC2401 al RFC2412 y R FC2451.

Movilidad

La posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad, es otra de las motivaciones básicas de IPv6. Como no, ya se han iniciado trabajos al respecto en IPv4, pero las complicaciones para usar la movilidad en este caso son enormes.
El documento base de estos trabajos es *draft-ietf-mobileip -ipv6-12.txt* . La idea básica permite identificar a un nodo móvil por su dirección de partida ("home address"), independientemente de su punto de conexión a Internet en cada momento dado. Por supuesto, cuando no esta en su punto de origen o de partida, también esta asociado con la información que permite identificar su posición o dirección actual ("care-of-address"). Los paquetes enviados a un nodo móvil (a su dirección de origen), son transparentemente enrutados a su "dirección actual".
El protocolo también permite que los nodos IPv6 almacenen la información de vinculación entre la dirección de partida y la posición actual, a modo de caché, y por tanto sean capaces de enviar los paquetes destinados al nodo móvil, directamente a su "dirección actual".
Para ello, el protocolo define nuevas opciones de destino, una de las cuales ha de ser soportada incluso en paquetes recibidos por todos los nodos (aunque no sean móviles).
Además, hay que prever, dada la estructura habitual de las redes inalámbricas (ejemplo muy habitual, la telefonía celular), que un nodo móvil puede estar conectado simultáneamente a varias redes (varías células que se solapan), y debe de ser alcanzable por cualquiera de ellas.
Los trabajos iniciales están documentados en el RFC2002 (soporte de movilidad en IP) y sucesivos. Además, se han publicado ya las especificaciones para túneles inversos en redes IP móviles (RFC2344), en cuya actualización se esta trabajando (draft-ietf-mobileip-rfc2344-bis-01.txt).
Se trabaja también en apartados como los requisitos de autenticación, autorización y facturación (draft-ietf-mobileip-aaa-reqs-03.txt), comúnmente denominadas AAA (Authentication, Authorization and Accounting), las extensiones de autenticación (draft-ietf-mobileip-challenge-09.txt), las claves de registro AAA (draft-ietf-mobileip-aaa-key-01.txt), la optimización de rutas (draft-ietf-mobileipoptim- 09.txt), claves de registro para la optimización de rutas (draft-ietf-mobileipregkey- 01.txt), registros regionales (draft-ietf-mobileip-reg-tunnel-02.txt), entre otros.

DNS (RFC1886)

El mecanismo fundamental por el cual nos referimos a direcciones IP para la localización de un host, es el uso de literales (URL), como ya hemos anticipado en apartados anteriores. Sin embargo, para que este mecanismo funcione, a más bajo nivel existe un protocolo denominado "Sistema de Nombres de Dominio" (Domain Name System o DNS).

Este mecanismo, definido para IPv4 (RFC1034 y RFC1035), fue actualizado por el RFC1886, básicamente incluyendo un nuevo tipo de registro para almacenar las direcciones IPv6, un nuevo dominio para soportar las "localizaciones" (lookups) basadas en IPv6, y definiciones actualizadas de tipos de consultas existentes que devuelven direcciones Internet como parte de procesos de secciones adicionales.

Las extensiones han sido diseñadas para ser compatibles con las aplicaciones existentes y, en particular, con las implementaciones del propio DNS.

El problema del sistema de DNS existente es fácilmente comprensible: Al hacer una consulta, las aplicaciones asumen que se les devolverá una dirección de 32 bits (IPv4). Para resolverlo, hay que definir las siguientes extensiones, antes indicadas:

Un nuevo tipo de registro de recurso para mapear un nombre de dominio con una dirección IPv6: Es el registro AAAA (con un valor de tipo 28, decimal). Un nuevo dominio para soportar búsquedas basadas en direcciones. Este dominio es IP6.INT. Su representación se realiza en orden inverso de la dirección, separando los nibbles (hexadecimal) por puntos ("."), seguidos de ".IP6.INT".

Así, la búsqueda inversa de la dirección 4321:0:1:2:3:4:567:89ab, seria "b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT" Redefinición de las consultas existentes, que localizan direcciones IPv4, para que puedan también procesar direcciones IPv6. Ello incluye TODAS las consultas, lógicamente (NS, MX, MB, ...).

Además, para soportar la agregación de direcciones IPv6, la renumeración y el multi-homing, se trabaja en un nuevo documento (draft-ietf-ipngwg-dnslookups- 07.txt), que incluye un nuevo tipo de registro de recurso (A6) para almacenar las direcciones IPv6 de forma que se agilice la renumeración de la red. Se prevé que este documento sustituya al RFC1886.

Otros documentos relevantes son: RFC2181 (clarificaciones a las especificaciones DNS), RFC2535 (extensiones de seguridad para DNS), RFC2672 (redirección de árboles DNS), RFC2673 (etiqueta binarias en DNS).

Protocolos de Routing

Básicamente se adoptan los mismo protocolos de enrutado que los existentes en las redes IPv4: RIP, OSPF y BGP. Pero además se está trabajando en IDRP (ISO Inter-Domain Routing Protocol) e IS-IS (Intermediate System to Intermediate System).

RIPng (RFC2080 y RFC2081)

La especificación del Protocolo de Información de Rutas (RIP – "Routing Information Protocol") para IPv6, recoge los cambios mínimos e indispensables al RFC1058 y RFC1723 para su adecuado funcionamiento.

RIPng es un protocolo pensado para pequeñas redes, y por tanto se incluye en el grupo de protocolos de pasarela interior (IGP – "Interior Gateway Protocol"), y emplea un algoritmo denominado "Vector-Distancia". Se basa en el intercambio de información entre routers, de forma que puedan calcular las rutas más adecuadas, de forma automática.

RIPng sólo puede ser implementado en routers, donde requerirá como información fundamental, la métrica o número de saltos (entre 1 y 15), que un paquete ha de emplear, para llegar a determinado destino. Cada salto supone un cambio de red, por lo general atravesando un nuevo router.

Además de la métrica, cada red tendrá un prefijo de dirección destino y la longitud del propio prefijo.

Estos parámetros han de ser configurados por el administrador de la red.

El router incorporará, en la tabla de enrutado, una entrada para cada destino accesible (alcanzable) por el sistema. Cada entrada tendrá como mínimo, los siguiente parámetros:

- El prefijo IPv6 del destino.
- La métrica (número de saltos entre este router y el destino).
- La dirección IPv6 del siguiente router, así como la ruta para llegar a él.
- Un indicador relativo al cambio de ruta.
- Varios contadores asociados con la ruta.
- Además se podrán crear rutas internas (saltos entre interfaces del propio router), o rutas estáticas (definidas manualmente).
- RIPng es un protocolo basado en UDP. Cada router tiene un proceso que envía y recibe datagramas en el puerto 521 (puerto RIPng).

El inconveniente de RIPng, al igual que en IPv4, siguen siendo, además de su orientación a pequeñas redes (diámetro de 15 saltos como máximo), en que su métrica es fija, es decir, no puede variar en función de circunstancias de tiempo
real (retardos, fiabilidad, carga, etc.).

OSPFv6 (RFC2740)

El protocolo de enrutado "Abrir Primero el Camino más Corto" (OSPF –"Open Shortest Path First"), es también un protocolo IGP (para redes autónomas), basado en una tecnología de "estado de enlaces" ("link-state").

Se trata de un protocolo de enrutado dinámico, que detecta rápidamente cambios de la topología (como un fallo en un router o interfaz) y calcula la siguiente ruta disponible (sin bucles), después de un corto período de convergencia con muy poco tráfico de routing.

Cada router mantiene una base de datos que describe la topología del sistema autónomo (de la red), y es lo que denominamos base de datos de "estado de enlaces". Todos los routers del sistema tienen una base de datos idéntica, indicando el estado de cada interfaz, y de cada "vecino alcanzable".
Los routers distribuyen sus "estados locales" a través del sistema autónomo (la red) por medio de desbordamientos ("flooding").
Todos los routers utilizan el mismo algoritmo, en paralelo, y construyen un árbol de las rutas más cortas, como si fueran la raíz del sistema. Este árbol de "rutas más cortas" proporciona la ruta a cada destino del sistema autónomo. Si hubiera varias rutas de igual coste a un determinado destino, el tráfico es distribuido equilibradamente entre todas. El coste de una ruta se describe por una métrica simple, sin dimensión.
Se pueden crear áreas o agrupaciones de redes, cuya topología no es retransmitida al resto del sistema, evitando tráfico de routing innecesario.
OSPF permite el uso de máscaras diferentes para la misma red ("variable length subnetting"), lo que permite el enrutado a las mejores rutas (las más largas o más específicas).
Todos los intercambios de protocolo OSPF son autenticados, y por tanto sólo pueden participar los routers verificados ("trusted").
OSPFv6 mantiene los mecanismos fundamentales de la versión para IPv4, pero se han tenido que modificar ciertos parámetros de la semántica del protocolo, así como el incremento del tamaño de la dirección. OSPFv6 se ejecuta basado en cada enlace, en lugar de en cada subred.
Además, ha sido necesario eliminar la autenticación del protocolo OSPFv6, dado que IPv6 incorpora estas características (AH y ESP).
A pesar de la mayor longitud de las direcciones, se ha logrado que los paquetes OSPFv6 sean tan compactos como los correspondientes para IPv4, eliminando incluso algunas limitaciones y flexibilizando la manipulación de opciones.

BGP4+ (RFC2283, RFC2545)

El Protocolo de Pasarelas de Frontera (BGP – "Border Gateway Protocol") es un protocolo de enrutado para la interconexión de sistemas autónomos, es decir, para el enrutado entre diferentes dominios.
Frecuentemente se emplea para grandes corporaciones y para la conexión entres proveedores de servicios (como ISP's).
Su principal función es, por tanto, el intercambio de información de disponibilidad o alcance entre varios sistemas BGP, incluyendo información de los sistemas autónomos que contienen, permitiendo así construir las rutas más adecuadas y evitar bucles de tráfico.
BGP4 incorpora mecanismos para soportar enrutado entre dominios sin clases ("classless interdomain routing"), es decir, el uso de prefijos, agregación de rutas, y todos los mecanismos en los que se basa IPv6.

BGP se basa en que un dispositivo sólo informa a los otros dispositivos que se conectan a él, acerca de las rutas que el mismo emplea. Es decir, es una estrategia de "salto a salto". La implicación es la simplicidad de Internet, pero la desventaja es que este mecanismo impide políticas complejas, que precisan de técnicas como el enrutado de fuente ("source routing").
BGP usa TCP como protocolo de transporte, a través del puerto 179.
BGP4+ añade a BGP (RFC1771), extensiones multiprotocolo, tanto para IPv6 como para otros protocolos, como por ejemplo IPX.

Estrategias de Transición (RFC1933)

La clave para la transición es la compatibilidad con la base instalada de dispositivos IPv4. Esta afirmación define un conjunto de mecanismos que los hosts y routers IPv6 pueden implementar para ser compatibles con host y routers IPv4.
Estos mecanismos permitirán usar infraestructuras IPv4 para IPv6 y viceversa, dado que se prevé que su uso será prolongado, e incluso indefinido en muchas ocasiones.

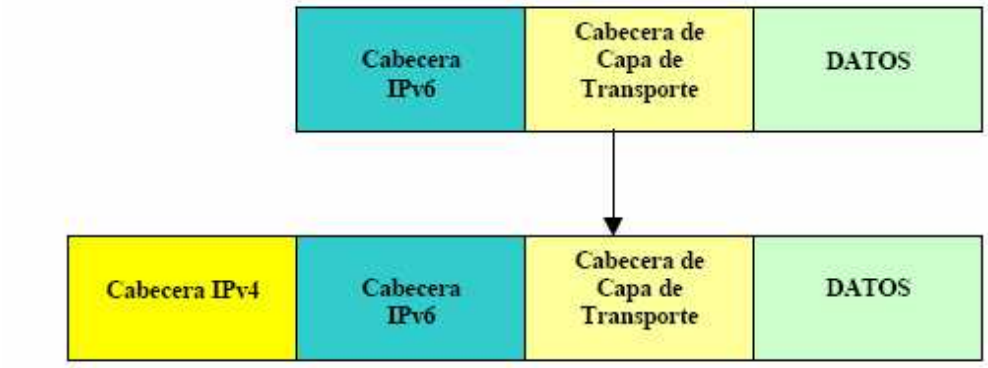
Doble pila (IPv4 e IPv6)

El camino más lógico y evidente de transición es el uso simultáneo de ambos protocolos, en pilas separadas. Los dispositivos con ambos protocolos también se denominan "nodos IPv6/IPv4".
De esta forma, un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos (nodos sólo IPv4 o sólo IPv6).
El dispositivo tendrá una dirección en cada pila. Se pueden utilizar direcciones IPv4 e IPv6 relacionadas o no, y se pueden utilizar mecanismos manuales o automáticos para la asignación de las direcciones (cada una correspondiente al protocolo en cuestión).
El DNS podrá devolver la dirección IPv4, la dirección IPv6, o ambas. Como ya hemos explicado en el apartado de direcciones especiales IPv6, se pueden emplear la dirección IPv4 (32 bits), anteponiéndole 80 bits con valor cero y 16 bits con valor 1, para crear una dirección IPv6 "mapeada desde IPv4".

Túneles IP v6 sobre IPv4

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 esta siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4.
Los extremos finales del túnel siempre son los responsables de realizar la operación de encapsulado del paquete/es IPv6 en IPv4.
Estos túneles pueden ser utilizados de formas diferentes:

Router a router. Routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.
Host a router. Hosts con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4.
El túnel comprende el primer segmento de la ruta seguida por los paquetes.
Host a host. Hosts con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.
Router a host. Routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la ruta.
Los túneles se clasifican según el mecanismo por el que el nodo que realiza el encapsulado determina la dirección del nodo extremo del túnel. En los dos primeros casos (router a router y host a router), el paquete IPv6 es tunelizado a un router. El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina "túnel configurado", describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado.
En los otros dos casos (host a host y router a host), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina "túnel automático".



El "desencapsulado", en el extremo final del túnel, realiza la función opuesta, lógicamente.

Transmisión de IPv6 sobre dominios IPv4 (RFC2529)

Este mecanismo permite a hosts IPv6 aislados, sin conexión directa a routers IPv6, ser totalmente funcionales como dispositivos IPv6.

Para ello se emplean dominios IPv4 que soportan multicast como su enlace local virtual. Es decir, usamos multicast IPv4 como su "ethernet virtual".
De esta forma, estos hosts IPv6 no requieren direcciones IPv4 compatibles, ni túneles configurados.
Los extremos finales del túnel se determinan mediante ND. Es imprescindible que la subred IPv4 soporte multicast.
Este mecanismo se denomina comúnmente "6 over 4".

Conexión de dominios IPv6 sobre redes IPv4

El documento draft-ietf-ngtrans-6to4-04.txt nos indica un mecanismo comúnmente denominado "6 to 4", para asignar un prefijo de dirección IPv6 a cualquier sitio que tenga al menos una dirección IPv4 pública.
De esta forma, dominios o hosts IPv6 aislados, conectados a infraestructuras IPv4 (sin soporte de IPv6), pueden comunicar con otros dominios o hosts IPv6 con una configuración manual mínima.
Este mecanismo funciona aún cuando la dirección IPv4 global (pública) es única y se accede a la red mediante mecanismos NAT (Network Address Translation), que es el caso más común en las redes actuales para el acceso a Internet a
través de ISP's.

"Tunnel Server" y "Tunnel Broker"

El documento draft-ietf-ngtrans-broker-02.txt sienta las bases para aplicaciones que permiten utilizar, de forma libre y gratuita, nuestras direcciones IPv4 actuales, sobre las infraestructuras IPv4, para acceder a redes y sitios IPv6.
Estos mecanismos se hacen indispensables para labores de investigación, dado que se requieren direcciones IPv6 y nombres DNS permanentes.
La diferencia con el mecanismo "6to4" es que el "Tunnel Broker" no requiere la configuración de un router.
Se trata de ISP's IPv6 "virtuales", proporcionando conectividad IPv6 a usuarios que ya tienen conectividad IPv4.
El "tunnel broker" es el lugar donde el usuario se conecta para registrar y activar "su túnel". El "broker" gestiona (crea, modifica, activa y desactiva) el túnel en nombre del usuario.
El "tunnel server" es un router con pila doble (IPv4 e IPv6), conectado a Internet, que siguiendo órdenes del "broker" crea, modifica o borra los servicios asociados a un determinado túnel/usuario.
El mecanismo para su configuración es tan sencillo como indicar, en un formulario Web, datos relativos al S.O., la dirección IPv4, un "apodo" para la máquina, y el país donde esta conectada. El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente.
Se pueden hallar ejemplos de estos sistemas en h t t p://www.freenet6.nety

http://carmen.cselt.it/ipv6/download.html.

Otros mecanismos de transición

Estas técnicas pueden ser utilizadas incluso de forma combinada.
aquí expuestos, a través de los borradores draft-ietf-ngtrans-mech-06.txt, draftietf-ngtrans-translator-03.txt, draft-ietf-ngtrans-socks-gateway-04.txt, draft-ietfngtrans-dstm-01.txt,draft-ietf-ngtrans-tcpudp-relay-00.txt,draft-ietf-ngtranshometun-00.txt y draft-ietf-ngtrans-ipv4survey-00.txt.
Un documento introductorio completo a todos los mecanismos es draft-ietfngtrans-introduction-to-ipv6-transition-03.txt.

Situación del estándar: RFC's y borradores

Los RFC's existentes son los siguientes:

	RFC	**DECRIPCION**
Especificaciones básicas	RFC2460	Especificaciones del Protocolo Internet Versión 6 (IPv6)
	RFC2461	Descubrimiento del Vecindario para IPv6 (ND)
	RFC2462	Autoconfiguración de Direcciones "stateless" IPv6
	RFC2463	Protocolo de Mensajes de Control de Internet para IPv6 (ICMPv6)
	RFC1981	Descubrimiento del MTU de la ruta para IPv6
	RFC1809	Uso del campo "Etiqueta de Flujo" en IPv6
Direccionamiento	RFC2373	Arquitectura de Direccionamiento en IPv6
	RFC1887	Arquitectura para la Asignación de Direcciones Unicast IPv6
	RFC2374	Formato de Direcciones Unicast Agregables Globales
	RFC2450	Propuesta de normas de asignación de TLA y NLA
Routing	RFC2080	RIP para IPv6
	RFC2081	Aplicabilidad de RIPng para IPv6
	RFC2283	Extensiones Multiprotocolo para BGP-4
	RFC2545	Uso de las Extensiones Multiprotocolo de BGP-4 para Routing entre dominios para
	RFC2740	OSPF para IPv6
DNS	RFC1886	Extensiones DNS para soportar IPv6
IP sobre..	RFC2464	Transmisión de paquetes IPv6 sobre redes Ethernet
	RFC2467	Transmisión de paquetes IPv6 sobre redes FDDI
	RFC2470	Transmisión de paquetes IPv6 sobre redes Token Ring
	RFC2472	IPv6 sobre PPP
	RFC2491	IPv6 sobre redes de Acceso Múltiple Sin Broadcast
	RFC2492	IPv6 sobre redes ATM
Seguridad	RFC2401	Arquitectura de Seguridad para IP
	RFC2402	Cabecera de Autenticación IP
	RFC2406	Encriptación de datos en IP (ESP)
	RFC2408	Asociaciones de Seguridad y Protocolo de Gestión de Claves en Internet (ISAKMP)
Multicast	RFC2375	Asignación de Direcciones Multicast
	RFC2710	Descubrimiento de nodos que desean recibir Multicast para IPv6
	RFC2776	Protocolo de Anunciación de Zonas de Ambito Multicast (MZAP)

Anycast	RFC2526	Direcciones de Subredes para Anycast en IPv6
Multi-homming	RFC2260	Soporte Escalable de Multi-homing para Conectividad Multi-Proveedor
	RFC2497	Transmisión de paquetes IPv6 sobre redes ARCnet
Transicion	RFC1933	Mecanismos de Transición para Routers y Hosts IPv6
	RFC2185	Aspectos de Routing de la Transición IPv6
	RFC2473	Especificaciones Genéricas de Tunelización de Paquetes en IPv6
	RFC2529	Transmisión de IPv6 sobre Dominios IPv4 sin Túneles Explícitos
	RFC2765	Algoritmo de Traslación Stateless IP/ICMP (SIIT)
	RFC2766	Protocolo de Traslación – Traslación de Dirección de Red
	RFC2767	Doble Pila en Hosts usando la Técnica "Bump-In-the-Stack" (BIS)
API	RFC2292/bis	Advanced Sockets API para
	RFC2553/bis	IPv6 Basic Socket API para IPv6
MIB	RFC2452	Base de Información de Gestión para IPv6: TCP
	RFC2454	Base de Información de Gestión para IPv6: UDP
	RFC2465	Base de Información de Gestión para IPv6: Convenciones Textuales y Grupo General
	RFC2466	Base de Información de Gestión para IPv6: ICMPv6
OTROS	RFC1881	Gestión de la Asignación de Direcciones IPv6
	RFC1924	Representación Compacta de Direcciones IPv6
	RFC2147	TCP y UDP sobre Jumbogramas IPv6
	RFC2428	Extensiones FTP para IPv6 y NAT
	RFC2471	Plan de Asignación de direcciones IPv6 para Pruebas
	RFC2474	Definición del Campo de Servicios Diferenciados (DS) en Cabeceras IPv4 e IPv6
	RFC2546	Prácticas de Routing en 6Bone
	RFC2663	Consideraciones y Terminología de IP NAT
	RFC2732	Formato para la representación literal de direcciones IPv6 en URL's
	RFC2772	Guías de Routing en el troncal 6Bone
	RFC2775	Transparencia de Internet

Pero además, se esta trabajando en los siguientes documentos (drafts):

	DOCUMENTO	DESCRIPCION
Direccionamiento	ipngwg-iana-tla-03.txt	Asignaciones Iniciales de Identificadores sub-TLA IPv6
	ipngwg-site-prefixes-04.txt	Prefijos de Sitios en ND
	ipngwg-esd-analysis-05.txt	Análisis de propuesta de direccionamiento GSE para IPv6
	ipngwg-scopedaddr-format-02.txt	Extensión de formato para Ambitos de Direcciones en IPv6
	ipngwg-scoping-arch-01.txt	Arquitectura de Ambitos de Direcciones en IPv6
	ipngwg-addr-arch-v3-00.txt	Arquitectura de Direccionamiento en IPv6
Routing	ipngwg-router-renum-10.txt	Renumeración de Routers para IPv6
	ipngwg-scoped-routing-04.txt	Routing de Ambitos de Direcciones en IPv6
DNS	ipngwg-dns-lookups-08.txt	Extensiones DNS para soportar Agregación y Renumeración en IPv6
ICMP	ipngwg-icmp-name-lookups-05.txt	Peticiones de información a nodos en IPv6
ND	ion-ipv6-ind-03.txt	Extensiones a ND en IPv6 para descubrimiento inverso
Movilidad	mobileip-ipv6-12.txt Soporte de Movilidad en IPv6	
	mobileip-challenge-12.txt	Extensiones de Desafío/Respuesta en movilidad IP
	mobileip-aaa-reqs-03.txt	Requisitos de Autenticación, Autorización y Contabilidad (AAA) en movilidad IP
	mobileip-rfc2344-bis-01.txt	Revisión de Túneles Inversos para movilidad IP
DHCP	dhc-dhcp-dns-12.txt	Interacción entre DHCP y DNS
	dhc-autoconfig-04.txt	Opción DHCP para desactivar la autoconfiguración stateless en clientesIPv4
	dhc-dhcpv6-15.txt	Protocolo de Configuración Dinámica de Host para IPv6 (DHCPv6)
	dhc-v6exts-12.txt	Extensiones para DHCPv6
Seguridad	ipngwg-addrconf-privacy-01.txt	Extensiones de Privacidad para Autoconfiguración de Direcciones Stateless en IPv6
	ipngwg-default-addr-select-00.txt	Selección de Direcciones por Defecto para IPv6
Multi-homming	ipngwg-ipv6multihome-with-aggr-00.txt	Multi-Homing en IPv6 con Agregación de Rutas
	ipngwg-multi-isp-00.txt	Problemática de dominios con Routing Multi-Homing en IPv6
Transición	ngtrans-translator-03.txt	Técnicas de Transición para comunicación entre IPv6 e IPv4
	ngtrans-mech-06.txt	Mecanismos de Transición para Host y Routers IPv6
	ngtrans-6to4-06.txt	Conexión de dominios IPv6 a través de redes IPv4 sin túneles explícitos
	ngtrans-broker-02.txt	Tunnel Broker para IPv6
	ngtrans-introduction-to-ipv6-transition-03.txt	Guía para la introducción de IPv6 en el mundo IPv4
	ngtrans-socks-gateway-04.txt	Mecanismos de Pasarela IPv6/IPv4 bas ados en SOCKS

	ngtrans-6bone-6papa-01.txt	Pre-cualificación para asignación de prefijos de direcciones en Bone (6PAPA)
	ngtrans-dstm-01.txt	Mecanismo de Transición de doble pila (DSTM)
	ngtrans-tcpudp-relay-01.txt	Traductor de relé de transporte IPv6-IPv4
	ngtrans-hometun-00.txt	Túneles IPv6 sobre IPv4 para acceso doméstico a Internet
	ngtrans-ipv4survey-00.txt	Inspección de direcciones IPv4 en normas actuales IETF
MIB	ipngwg-mld-mib-03.txt	Base de Información de Gestión para Multicast Listener Discovery Protocol en IPv6
OTROS	pim-ipv6-03.txt	Protocolo de Routing Multicast Independiente en IPv6 Otros
	pim-v2-sm-01.txt	Protocolo de Routing Multicast Independiente en Modo Esparcido (PI