UNIVERSIDAD ADVENTISTA DE CENTROAMERICA

PROTOCOLO DE INTERNET VESION 6

Presentado en requisito a la materia:

TELEMATICA Y REDES

Profesor:

Lic. Jair del Valle

Realizado por:

Jorge Rivera

Alajuela, Costa Rica.

INDICE.

Introduccion I

El mundo de los sue~os primero se penso en una increible red, que se extendiera rapidamente por todo el planeta y lograra conectar tantas computadoras como fuese posible, una red que tuviera vida propia y que fuese la casa del conocimiento y la libertad. William Gibson comenzo a impresionar a sus lectores con terminos extra~os tales como ciberespacio y realidad virtual, las ideas de mundos virtuales en los que los humanos y entes IA se conocen e interactuan; un mundo sin limites donde flotan las fantasias reales. Esto era considerado por la gente normal como ficcion cientifica. La realidad en estas epocas solo estaba en la imaginacion. Internet fue el paso mas acertado para que esa imaginacion fuese explotada.

Introduccion II

Debido a la inauguracion de los laboratorios de InET, he decidido hacer un articulo acerca del nuevo protocolo de IP denominado IPv6. Mi deseo es hacer una serie de varios tomos con este tema, en el cual se explique a fondo las caracteristicas de este nuevo protocolo; asi que comienzo con la introduccion y en la proxima entrega explicare lo que es meramente tecnico.

Para un mejor entendimiento del articulo es necesario tener bases del protocolo TCP/IP. Si no sabes mucho... que esperas para aprender?, ve ya mismo a bajarte un manual de TCP/IP antes de leer lo que viene (Ahhh, estoy exagerando, mejor leelo y si te quedan dudas te bajas el manual... bien?)

Introduccion III

Dentro de las caracteristicas tecnicas que crean una comunicacion basada en el intercambio de paquetes, se encuentra la direccion IP.

Las primeras organizaciones encargadas del desarrollo de internet (todo esto no tiene que ver con los hackers, que son sus fundadores) se preocupaban por seleccionar un tipo de protocolo estandar para efectuar las operaciones de intercambio de paquetes. Esto ocasiono un ambiente competitivo muy desagradable entre distintas compa~ias que querian tener el credito de ser las primeras en implementar el protocolo ideal para la comunicacion en internet.

Nombres como CLNP (Conection-Less network Protocol), TUBA (TCP and UDP OverBigger Adresses), TP/IX, SIP (Simple IP) e IPv4 son los protocolos que han influido de una u otra forma al desarrollo de internet. Al principio se pensaba que internet no iba a ser una red a la cual millones de usuarios iban a acceder. por eso actualmente se trabaja con el protocolo IPv4, un protocolo de comunicacion eficiente pero con el defecto de tener muy limitado sus bits de direcciones de red, lo cual hace que el cupo de las computadoras conectadas a internet sea muy limitado (esto me hace acordar del peque~o descuido del a~o 2000...en fin, cuestiones apocalipticas aparte ;)).

Este protocolo ha sido implementado desde hace ya mas de veinte a~os, pero ya esta llegando a su fin. Dentro de los problemas que se destacan en el esta la incapacidad de tener incorporada dentro de su propia arquitectura la encriptacion de paquetes y seguridad (Ipsec), el servicio DHCP (Dynamic Host Configuration Protocol), NAT (Network Adress Translator) y la limitacion de direcciones a 32 bits. (a diferencia del Ipv6 que utiliza direcciones a 128 bits). El protocolo IPv6 se destaca por implementar la tecnologia Ipsec (la cual sera una adicion del protocolo IPv4 en el desarrollo de la seguridad) y el DHCP (Dynamic Host Configuration Protocol) que es el servicio que permite la autoconfiguracion de direcciones IP disponibles, en este caso sin necesidad de un servidor, todo mediante la autoconfiguracion sin estado.

Las direcciones de IPv6 aumentan en una cantidad de 1028 veces mas que las de IPv4; gracias al nuevo esquema agregado de direcciones, los 48 bits a la izquierda de la direccion asignada constituyen la ruta . publica. El primer campo (conformado por 3 bits) indica que el formato de direcciones es agregado. El segundo campo indica la identidad del agregador de nivel mas alto el cual se limita a 8192 proveedores de alto trafico. El tercero esta conformado por los agregadores de proximo nivel que permiten la alineacion jerarquica para la existencia de varios subniveles de ISP. El cuarto es el agregador de nivel de sitio para la organizacion de los propios subniveles y el ultimo es el identificador de interfaz en el cual se almacena el codigo de la compa~ia y el identificador de extension. Todo esto se explicara detalladamente en futuras entregas.

En la actualidad existe un banco de pruebas internacional encargado de las operaciones necesarias que se deben implementar en el protocolo IPv6 para su correcto funcionamiento en un futuro, su nombre es 6Bone.

Dentro de su anatomia basada en tuneles de trafico sobre la infraestructura IPv4 existente se encuentran caracteristicas como las pilas dobles de trafico IPv4 - IPv6 y viceversa para el envio libre del IPv6 sobre internet; el IPv6 encapsulado en paquetes IPv4; un DNS que soporta registros AAAA de IPv6; un registro de la ruta 6bone que controle los puntos de servicio y sus tuneles y soporte al publico por medio de una lista de correo y una pagina web (http://www.6bone.net). El desarrollo del protocolo IPv6 crece de acuerdo a la colaboracion de diferentes organizaciones que se unan voluntariamente al banco de pruebas 6Bone.

Si alguien esta interesado en la configuracion de IPv6 y usa Linux pues que esta esperando... aqui les presento una peque~a guia de configuracion para Linux (eso si, peque~a... esto es una introduccion)

- La instalacion de la configuracion primaria es almacenado en /etc/sysconfig/network-ip6

-> Aqui puedes especificar un nivel de debug para los scripts de IPv6
- Activa/desactiva la interface de configuracion IPv6 y especifica un archivo de informacion.
- Activa/desactiva la configuracion de Enrutamiento/Puerta de Enlace y especifica un archivo de informacion.
- Activa/desactiva el IPv6 forwarding, este debe estar activado en un host para actuar como un router
- Activa/desactiva la configuracion de tunel IPv6 y especifica un archivo de informacion.
- Activa/desactiva el IPv6 radvd y especifica el archivo de configuracion y algunas opciones con los demonios.

Ejemplo: network-ip6

```
#!F:network-ip6
#
#!P:/etc/sysconfig
#
#!D:IPv6 network configuration file
#
#!C:Copyright 1997-1998 Peter Bieringer <pb@bieringer.de>
#
#!V:Version 1.11 05.03.1998

# Changes to:
#  1.11: add IP6FORWARDING switch (to differ between a host and a router)


## IPv6 configuration debugging
# Bit0: show all commands, bit1:don't execute anything
IP6DEBUG=0

## IPv6 network configuration? {yes|no}
IP6NETWORKING=yes
#IP6NETWORKING=no

# Take information from the file
IP6INTERFACEFILE=/etc/sysconfig/network-ip6.conf


## Gateway network configuration
# for i.e. routing IPv6 packages over local IPv6 routers
# similar to the default gateway in IPv4)

# Allow gateway configurations {yes|no}
IP6GATEWAYCONFIG=yes
```

#IP6GATEWAYCONFIG=no

# Take information from the file
IP6ROUTEFILE=/etc/sysconfig/network-ip6.conf

# Allow forwarding option, host is a router {yes|no}
IP6FORWARDING=yes
#IP6FORWARDING=no

IPv6 tunnels
for tunneling IPv6 packages over IPv4 routers to a IPv6 tunnel endpoint
i.e. 6bone connection, ask a 6bone partner near your location for set up
tunnel to you

# Allow IPv6 tunnel interface configuration {yes|no}
IP6TUNNELCONFIG=yes
#IP6TUNNELCONFIG=no

# Take information from the file
IP6TUNNELFILE=/etc/sysconfig/network-ip6.conf

Router Advertisement Daemon
# Start Daemon {yes|no}
IP6RADVD=yes
#IP6RADVD=no

Sepcify configuration file
#IP6RADVDFILE="/usr/inet6/etc/radvd.conf"
IP6RADVDFILE="/etc/sysconfig/radvd.conf"

# Specify options
IP6RADVDOPTIONS=""
#IP6RADVDOPTIONS="-d 9"

-> Los valores de configuracion de la interface son guardados por ejemplo
en /etc/sysconfig/network-ip6.conf
- Este archivo esta especificado por las entradas en /etc/sysconfig/network- ip6
- La informacion en este archivo puede ser dividida en varios archivos
- Aqui puedes:
- Especificar varias direcciones IPv6 para cada interface.

- Especificar varias rutas de IPv6 por medio de Gateways (puertas de enlace) para cada interface.
- Especifica varios tuneles IPv6 a terminales de tuneles exteriores y tambien varios enrutamientos por medio de estos tuneles.
  - Ejemplo: network-ip6.conf

```
#!F:network-ip6.conf
#
#!P:/etc/sysconfig
#
#!S:root:root 440
#
#!D:IPv6 configuration file
#
#!C:Copyright 1997-1998 Peter Bieringer <pb@bieringer.de>
#
#!V:Version 2.12 16.05.1998

# Changes to
#  2.11: nothing important
#  2.12: NBMA tunnel configuration ready


# This file is needed by 'functions-ip6' version 2.xx

### The order in the file is only for a good overview, it is not really
### necessary. The important values are 'device' and 'key'!


################## Tunnel section

## Here you can configure tunnel endpoints. Be sure, that you set the device
## entry in a right way like 'sit1', 'sit2' and so on, otherwise you will get
## an error information from 'functions-ip6'

#Device Key                IPv4 gateway address
#sit1   tunnel             137.193.227.41
#sit2   tunnel             IPv4-Address
#sit3   tunnel             IPv4-Address


# Tunnel route section
# Here you can specify several routes to your configured tunnels.
# More than one are possible!
```

```
#Device Key                    Network
#sit1   route                  3ffe::/16
#sit2   route                  IPv6-Network/Prefix
#sit3   route                  IPv6-Network/Prefix

## Here you can configure tunnel endpoints in NBMA style. It's useful
for
## setting up many tunnels at once.

#Device Key     IPv4 gateway address    Network
sit     nbma    137.193.227.41          3ffe::/16
#sit    nbma    IPv4-Address            IPv6-Network/Prefix
#sit    nbma    IPv4-Address            IPv6-Network/Prefix

################## Interface section

## Here you can specify several addresses for your interfaces.
## More than one are possible!

#Device Key     prefix                  suffix          length
eth0    iface   fec0:0:0:1              0:0:0:1         64
eth0    iface   3ffe:0400:0100:f101     0:0:0:1         64

################## Gateway section

## Here you can specify several routes to your gateway.
## More than one are possible!

#Device Key     Gateway address                 Network
eth0    route   fec0:0:0:1:0:0:0:20             fec0:0:0:2::/64
eth0    route   3ffe:0400:0100:f101:0:0:0:20
3ffe:0400:0100:f102::/64
```

Para que entiendan mejor las caracteristicas de este protocolo, hare una comparacion entre el IPv6 y el SSL (Secure Sockets Layer). Los aspectos de la encriptacion usados en el IPv6 se trataran a fondo en la InET Magazine 4.

Basandonos en las especificaciones del IP secure, mas las caracteristicas incorporadas en el protocolo (algunas de las cuales

necesitan ser adiciones para el IPv4) sacamos ciertas conclusiones que nos sirven para compararlos: el IPv6 y el SSL no tienen cifrados restringidos, estan abiertos al publico en general. Ambos usan como algoritmos estandar el DES CBC (en realidad es un algoritmo muy vulnerable al crackeo, juego de ni~os para cualquier cypherpunk) pero se piensa en actualizar los algoritmos estandar de estos protocolos para incrementar su seguridad (3DES podria ser el algoritmo estandar).
SSL es usado para los servicios de host a host, o host a servidor, mientras que el IPv6 es mas profundo al emplearse en los servicios de host a subnet o entre dos subnets (que es el mas usado). SSL es un protocolo de transporte de capas, mientras que el IPv6 esta dentro de la capa de una red, haciendo que TODOS los paquetes que pasen por la red sean controlados por la seguridad del mismo protocolo, en cambio el SSL solamente se encarga de los protocolos SMTP, HTTP y NNTP. IPv6 brinda confidencialidad en la informacion y presta un buen servicio para autentificacion a todo el paquete IP, no solo a los valores de carga. (entonces... quedaran obsoletos los ataques IP spoofing??). El IPv6, con la capacidad que tiene en el encabezado de ruta puede hacer mas dificiles los intentos remotos de analisis de trafico en una red.

IPv6 demuestra gran potencia sobre el SSL, pero gracias a las aplicaciones basadas en browser para comercio electronico o transacciones seguras en general y al incorporarse facilmente a navegadores como el Netscape Navigator, el SSL se seguira utilizando durante mas tiempo.

Hasta aqui llega la primera entrega. !esto es solo una introduccion!

En el proximo numero de InET entraremos a explorar los aspectos tecnicos misteriosos del IPv6 y nos centraremos en la seguridad de y criptografia de este nuevo protocolo.

¿Qué es el IPv6?

IPv6 es una abreviatura de Internet Protocol, versión 6. Ésta emergente tecnologia es también conocida como IPng (pronunciado "I-Ping"), abreviatura de Protocolo de Internet, próxima generación.

IPv6 es un nuevo sitema, actualmente bajo desarrollo, que será usado en un futuro para asignar direcciones IP. Un consenso del IETF (Internet Engineering Task Force) determinó que el IPv6 será el sistema para la próxima generación de direcciones IP.

Eventualmente IPv6 remplazará el actual escenario de direccionamiento del Protocolo de Internet, conocido como IPv4.

¿Qué es el IPv6?

Una dirección IP (Internet Protocol) es un número que identifica a la computadora conectada en Internet.

Cada computadora conectada a Internet debe tener una única dirección IP.

¿Qué es el IPv6?

Actualmente, una dirección IP consiste en 4 secciones separadas por puntos. Cada sección contiene un valor de 8-bit representado con un

número entre 0 y 255. Tambien se lo conoce como direccionamiento de 32-bits.

Por ejemplo: 198.41.0.52

En este esquema, existen más de 4 billones de direcciones IP posibles. Sin embargo, la asignación de estas direcciones IP sigue una arquitectura de dos niveles que asigna numeros IP a una red y a los servidores de dicha red. Esta arquitectura mostro ser un método ineficiente para asignar espacios de direcciones IP y llevo a la idea de que a Internet se le agotaran las direcciones IP eventualmente.

¿Qué es el IPv6?

IPv6 usará direcciones IP de 128 bits. En este esquema, una dirección IP consistirá de 8 secciones, cada una conteniendo un valor de 16 bits. El número de direcciones IP posibles con este esquema es igual al del IPv4 al cuadrado, el doble.

La sintasis general para las nuevas direcciones IP es tener valores de direcciones IP separados por dos puntos. Por ejemplo:

1080:0:0:0:8:800:200C:417A

¿Qué es el IPv6?

La ventaja del IPv6 no esta solamente en su gran espacio de direcciones, sino tambien en su flexible arquitectura. IPv6 esta siendo diseñada para permitir el futuro crecimiento de la tecnologia de redes y expansion de Internet.

Existen actualmente planes para tres grandes tipos de direcciones IP. Cuando se implemente el IPv6, seran utilizadas aproximadamente el 15% del espacio de direccionamiento. Restando el 85% de espacio de direccionamiento, reservados para futuros usos.

El InterNIC (Internet Network Information Center), RIPE (Réseaux IP Européens), y APNIC (Asian-Pacific Network Information Center) estan trabajando en ediciones de asignaciones para el IPv6.

¿Qué es el IPv6?

La major característica del IPv6 es que sera totalmente compatible con el actual sistema de direccionamiento IPv4.

La transición desde el actual esquema de direcciones IP al IPv6 se espera que lleve varios años, pero dado que los dos sistemas son compatibles, la transición sera relativamente suave.

¿Qué es el IPv6?

El IPv6 esta actuamente bajo prueba. Una prueba de red IPv6, llamada "6Bone", conecta actualmente Norte America, Europa y Asia.

Especialistas en Internet estiman que Proveedores de Servicios de Internet comezaran a ofrecer vinculos IPv6 entre ahora y el fin de siglo.

¿Qué es el IPv6?

Sumario:

IPv6 es la abreviacion de Internet Protocol, version 6. IPv6 es un nuevo sistema, actualmente bajo desarrollo, para asignar direcciones

IP en el futuro. IPv6 reemplazara eventualmente el actual sistema de direccionamiento IP, conocido como IPv4.

IPv6 usara direcciones IP de 128 bits de largo. Con este esquema, una direccion IP consistira de 8 secciones, cada una conteniendo un valor de 16 bits. El numero de direcciones IP que esta crea es igual al espacio de direccionamiento del IPv4 al cuadrado, dos veces. IPv6 esta siendo diseñada para permitir el futuro crecimiento de la tecnologia de redes y expansion de Internet.

El Protocolo de Internet versión 6 *(Internet Protocol Version 6, IPv6)* es el nivel más reciente del protocolo de Internet (IP) y actualmente se incluye como parte del soporte IP en muchos productos incluyendo los principales sistemas operativos de ordenador. El IPv6 ha sido llamado "IPng" (IP siguiente generación o Next Generation). Formalmente, el IPv6 es un grupo de especificaciones de la Fuerza de Tarea de Ingeniería de Internet (Internet Engineering Task Force, IETF). El IPv6 se diseñó como un grupo de mejoras evolutivas a la actual versión 4 del IP Version 4. Los hosts de red y los nodos intermedios ya sea con IPv4 o IPv6 pueden manejar paquetes formateados para cualquier nivel del Protocolo Internet. Los usuarios y proveedores de servicio pueden actualizarse al IPv6 independientemente, sin tenerse que coordinarse entre sí.

La más obvia mejora en el IPv6 sobre el IPv4 es que las direcciones IP se alargan de 32 a 128 bits. Esta extensión anticipa un considerable crecimiento futuro de Internet y proporciona un alivio a lo que se consideraba una inminente escasez de direcciones de red.

El IPv6 describe reglas para tres tipos de dirección: unicast (de un host a otro), anycast (de un host al más cercano de varios hosts), y multicast (de un host a múltiples hosts). Otras ventajas del IPv6 son:

- Se especifican opciones en una extensión al encabezado que sólo se examina en su destino, acelerando así el rendimiento general de la red.

- La introducción de una dirección "anycast" proporciona la posibilidad de enviar un mensaje al más cercano de varios hosts de puerta posibles con la idea de que cualquiera de ellos puede administrar el envío del paquete a otros. Los mensajes anycast pueden usarse para actualizar tablas de routing durante el proceso.

- Los paquetes pueden identificarse como pertenecientes a un "flujo" particular de modo que a los que son parte de una presentación de multimedia que tiene que llegar en "tiempo real" se les pueda proporcionar una mayor calidad de servicio (quality-of-service) comparados con otros clientes.

- El encabezado IPv6 ahora incluye extensiones que permiten que un paquete especifique un mecanismo para autenticar su origen para asegurar la integridad de los datos y la intimidad.

IP Versión 6:
La Próxima Generación del Protocolo Internet

A pesar de que la explosión del interés público por Internet data de 1994, el núcleo tecnológico sobre el que se sustenta, vale decir la familia de protocolos TCP/IP, cuenta ya con la respetable edad de un cuarto de siglo, tal como se reseña en el capítulo Internet: Historia y Orígenes Remotos, en este mismo servidor.

IP v4

Desde entonces, y particularmente desde principios de la década de los 90, este conjunto de protocolos ha soportado con éxito una carga de trabajo enormemente superior a la prevista por sus creadores, lo que

demuestra que se trató de un diseño tan robusto como versátil.

Sin embargo, y por virtud de la paradoja, ha sido el propio éxito de la actual versión de los protocolos TCP/IP, denominada IP v4, el factor que ha develado sus limitaciones, al punto de que algunos pronósticos agoreros se solazan en la visión de un apocalíptico colapso de Internet.

En rigor, de persistir las actuales tasas de crecimiento y de no mediar las oportunas medidas correctivas, ese futuro se plantearía como una ominosa posibilidad dentro de unos 15 años, particularmente en lo que se refiere al agotamiento del actual sistema de asignación de direcciones IP.

Básicamente, el problema remite a la estructura de direccionamiento de IP v4, compuesta por un esquema de 4 bytes, o 32 bits, y al sistema de asignación de direcciones, que definió tres tipos de redes:

Tipo de Redes	**Byte de Identificación**	**Nº de Identificación**	**Nº de Redes y Direcciones IP Posibles**
Clase A	Primer byte	entre 1.0.0.0. y 127.0.0.0	127 redes, c/u con espacio para 16.777.216 direcciones IP
Clase B	Dos primeros bytes	entre 128.0.0.0. y 191.0.0.0	16.320 redes, c/u con espacio para 65.024 direcciones IP
Clase C	Tres primeros bytes	entre 192.0.0.0 y 223.255.255.0	alrededor de dos millones de redes, c/u con espacio para 255 direcciones IP

Por más que se optimice por la vía administrativa el de suyo ineficiente sistema actual de asignación de direcciones IP, denominado Internet's global Domain

Name System (DNS), se calcula que a las actuales tasas de crecimiento, éste colapsaría entre los años 2.005 y 2.011; sin perjuicio de otros problemas no menos relevantes, relativos al enrutamiento y las tablas de rutas.

IP ng

Anticipándose a ese desenlace, ya en 1992 el IETF (Grupo de Trabajo Especial de Ingeniería Internet), convocó a la comunidad de investigadores en trabajo de redes a formar grupos de trabajo para estudiar distintas alternativas de solución al problema.

Nº de versión IP	Denominación
0-3	No asignado
4	Internet Protocol (actual)
5	ST (Stream Protocol)
6	SIP-SIPP-IP v6
7	IP v7- TC/IX-CAT NIP
8	Pip
9	TUBA
10-15	No asignado

Con el objeto de prevenir posibles conflictos de intereses, el IAB

(Internet Architecture Board) generó un documento con las especificaciones y requerimientos que debía reunir el próximo protocolo, al que se denominó genéricamente IP ng (next generation). Aunque parece similar, no debe confundirse con Next Generation Internet Initiative.

De hecho, diversos grupos de trabajo desarrollaron varias versiones del próximo Internet Protocol, como se detalla en la tabla adjunta.

En julio de 1994, el IAB resolvió formalmente que el IP v6 será el protocolo internet de la próxima generación. Esta familia de protocolos incluye desarrollos de IPAE, SIP, Pip y SIPP (Simple IP Plus).

IP v6

En principio, IP v6 conserva la mayor parte de las características y conceptos de operación de IP v4. Sin embargo, agrega nuevas capacidades y funcionalidades que permiten no sólo flexibilizar, sino que modelar nuevos conceptos de operación. Por de pronto, resuelve definitivamente el tema del número de direcciones IP, lo que no es poco decir.
Entre las principales características, de IP v6, cabe consignar:

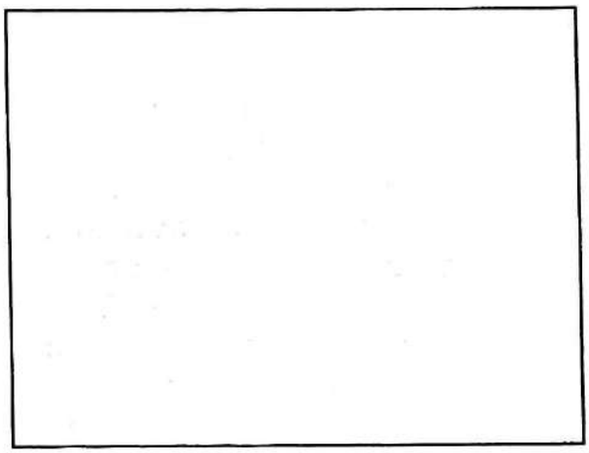
- **Expansión de direcciones:**
El incremento del rango de direcciones desde 32 a 128 bits, significa disponer sobre 3,4 x 10 elevado a 38 números posibles, es decir, una cantidad virtualmente ilimitada de direcciones IP. Esto significa que se podrá dar cabida no sólo a todos los nodos y computadores que lo requieran, sino también a dispositivos que en un futuro puedan entrar a la red, como por ejemplo, los televisores.
- **Simplificación del encabezamiento:**
IP v6 utiliza encabezamientos adicionales, de forma que provee opciones adicionales de operación, y proporciona un sistema más flexible para agregar capacidades y mecanismos adicionales a los datagramas, o paquetes de datos.
- **Mejoría de la calidad de servicios:**
IP v6 provee capacidades para administrar flujos de datagramas relativos a servicios particulares, los cuales pueden recibir un tratamiento diferenciado o preferencial, lo que garantiza un mejor nivel de comunicación para estos servicios.
- **Mejoría de los mecanismos de seguridad:**
IP v6 mejora la capacidad para la habilitación de

servicios seguros, mediante la ampliación y optimización de los mecanismos de identificación de datagramas y confidencialidad.

La implementación de IP v6 implica una modificación en computadores, routers (sistemas encaminadores) e, incluso en las aplicaciones, en una transición que no será sencilla; no obstante lo cual el usuario no tendrá que cambiar su dirección de correo electrónico o el URL de un Servicio de Información Web, puesto que los cambios se producen a nivel de los dominios de sistema.
Se estima que la migración masiva hacia el IPv6 puede comenzar en 1998.

Otros servidores con información relevante sobre el

- IP v6 de la NAS (Numerical Aerospace Simulation Facility) de la NASA.
- IP Next Generation (IPng) Information, de IETF (Internet Engenering Task Force).
- The Recommendation for the IP Next Generation Protocol
- Internet Protocol, Version 6 (IPv6) Specification to Proposed Standard, de la IESG (Internet Engineering Steering Group).
- Transition Mechanisms for IPv6 Hosts and Routers
- IP Next Generation Overview, de Robert Hinden.
- 6bone Home Page



Desarrollo de una Herramienta Software para el Acceso a Redes TCP/IP a través de la Red Telefónica Conmutada

Apéndice C:
IPng (IPv6)

IP *"next generation"* ha sido el nombre con el que se ha bautizado a la versión seis del protocolo Internet (IP). Se trata de la definición de

un nuevo protocolo de red destinado a sustituir a la actual versión IP, la cuatro.

¿Por qué se necesita un nuevo protocolo de red?. La respuesta es muy simple. Cuando IPv4 fue estandarizado, hace unos quince años, nadie podía imaginar que se convertiría en lo que es hoy: una arquitectura de amplitud mundial, con un número de usuarios superior al centenar de millones y que crece de forma exponencial. Aquella primera *"Internet"* fundada, sobre todo, con fines experimentales, científico-técnicos y, por supuesto, con objetivos militares, no se parece en nada a la actual. Cada día se advierte una mayor tendencia hacia su comercialización, ya sea por el propio acceso en sí a la red (empresas proveedoras) o por servicios accesibles desde ella.

Estos cambios de escala y orientación suponen varios problemas para IPv4 [RFC1287] [RFC1338] [RFC1917]:

- ***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 la pasarelas (routers) y el tráfico de gestión preciso para mantener sus tablas de encaminamiento. Existe un límite tecnológico al número de rutas que un nodo puede manejar, y como dado que Internet crece mucho más rápidamente que la tecnología que la mantiene, se vió 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.

Dado lo grave de la situación se definió el ***CIDR*** (*Classless Inter-Domain Routing*) [RFC1481] [RFC1517..1519], con el que las pasarelas reducían el tamaño de sus tablas colapsando juntas varias subredes con el mismo prefijo. Gracias a ello se ha ganado un tiempo muy valioso, pero tan sólo se ha postergado lo inevitable.

En [RFC1797] y [RFC1879] se realiza el experimento de dividir una red A (la red 39) en multitud de pequeñas subredes. Los resultados fueron alentadores, por lo que dicha técnica podría utilizarse para ampliar de nuevo el tiempo de vida de IPv4.

- ***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 a 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, etc., 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 a efectuar, el tiempo de permanencia en la red, etc. Cuando la red pertenece a una única organización eso es lo ideal, 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 qué redes desea que pasen sus datagramas, atendiendo a criterios de fiabilidad, coste, retardo, privacidad, etc. [RFC1674..1675].

A lo largo de los años se han propuesto varios protocolos como sustitutos al IPv4. Los tres más importantes han sido ***PIP*** (*'P' Internet Protocol*) [RFC1621] [RFC1622], ***TUBA*** (*TCP/UDP With Bigger Addresses*) [RFC1347] [RFC1526] y ***SIP/SIPP*** (*Simple Internet Protocol/Simple Internet Protocol Plus*) [RFC1710]. En [RFC1454] se realiza una buena comparativa entre ellos.
En 1.993 se decidió solicitar opiniones sobre *"cómo debería ser"* el IP del futuro (IPng) a través de [RFC1550]. Las respuestas recibidas fueron numerosas y provenientes de fuentes muy diversas. En general todas coincidían en los puntos básicos mencionados previamente. Tal vez los más interesantes hayan sido los que

mostraban el punto de vista de varias multinacionales [RFC1669] [RFC1684].

Por fin se propuso un estándar en 1.995 [RFC1752], refinado a principios de 1.996 en [RFC1883]. Como puede verse se trata de un tema de máxima actualidad. De hecho todavía faltan por publicar, al menos, dos funciones adicionales: *configuración dinámica* y *búsqueda de máquinas vecinas*. Los datos de que dispongo son de finales de Abril de 1.996 así que es muy posible que ahora, Junio, se hayan publicado algunos documentos adicionales.

Las principales características del nuevo IPv6, como diferencias respecto a IPv4, son [RFC1883]:

- Se trata de un protocolo diseñado para ser ampliado, de forma simple, con funcionalidades adicionales, ya sea a través de nuevas cabeceras de extensión o bien de opciones incluidas en las cabeceras ya existentes.
- Los nuevos números IP constan de 128 bits, lo cual permitirá efectuar una división muy jerárquica del espacio de direcciones para facilitar el enrutado. Adicionalmente ello posibilitará incluir la dirección física de la interfaz de red de la máquina en la propia dirección IP, facilitando de forma considerable el proceso de autoconfiguración.
- Se codifica directamente en el datagrama qué acción debe adoptar una máquina cuando ésta no es capaz de reconocer alguna de las opciones del mismo.
- Se incluyen cabeceras destinadas a la autentificación y la encriptación de los datagramas.
- Se permite que la fuente encamine directamente sus datagramas, como soporte a su política o necesidades de rutado.
- Los datagramas ya no tienen un límite de longitud de 65536 bytes.
- El soporte de encapsulados es muy natural, dado su diseño de cabeceras encadenadas.
- La fragmentación, en caso de ser necesaria, la realiza la fuente. Para facilitar el cálculo del MTU [RFC1191] [RFC1435] del camino hace falta el apoyo de la nueva capa ICMP [RFC1885]. Ahora, cuando una pasarela genera un mensaje ICMP *"Datagram Too Big"*, indica cuál es el MTU de la red problemática.
- La gestión de *Multicasting* [RFC966] [RFC988] [RFC1112] y *Anycasting* [RFC1546] (IGMP) ha pasado a formar parte del nuevo ICMP [RFC1886].
- Para acelerar el cálculo de los enrutamientos y atender las necesidades de las aplicaciones en tiempo real, cada datagrama puede contener un *"identificador de flujo"*. Esos identificadores son, en cierta medida, equivalentes al concepto de circuitos virtuales, pero se trata de unos circuitos virtuales *"suaves"* que

pueden ser desde ignorados hasta completamente vinculantes, según el diseño del sistema. Ello da un juego enorme. En mi opinión, éste es el concepto más novedoso e importante de IPv6 [RFC1809].

- IPv6 no incluye una suma de control en la cabecera. Para asegurar la validez de la información la capa UDP está obligada a utilizar su opción de suma de control. Adicionalmente el nuevo ICMP también incluye una suma de control, por razones similares.

Las nuevas direcciones IP, como ya se ha dicho, constan de 128 bits. Ello hace que la notación *"punto"* común de IPv4 sea poco práctica. IPv6 utiliza notación hexadecimal en grupos de 16 bits, separándolos por el carácter de dos puntos (**":"**) [RFC1884]. En [RFC1920] se propone una codificación más compacta.

En [RFC1884] se realiza una asignación preliminar de direcciones, muy agresiva. Se reserva una enorme cantidad de valores para determinados grupos de direcciones (por ejemplo, *multicasting*, NSAP (OSI), etc.), pero aún así el espacio disponible para usos todavía no especificados es del 85%. Las propias direcciones IPv4 están incluidas aquí. Hay varias novedades interesantes, como el hecho de definir direcciones especificamente locales a nivel de capa de enlace (MAC) u organización.

En definitiva, el IPv6 ya está aquí. Todavía queda un largo trecho hasta que se implante de forma mayoritaria, pero sin duda incorpora numerosas características que lo hacen atractivo, como el soporte de comunicaciones en tiempo real, la autoconfiguración de sistemas, seguridad, etc. La mayoría de los detalles todavía se están ultimando y, hasta donde sabe el autor, no se han propuesto aún plazos de implantación.

IPv6

A partir de un momento dado, a principios de la década de los 90, comenzó a estar claro que la última revisión del protocolo IP [RFC791], conocida como versión 4, no podría seguir prestando servicio durante mucho más tiempo, y una simple revisión del mismo no conseguiría solucionar los problemas existentes.

La arquitectura de direcciones del protocolo se estaba convirtiendo en un serio problema. La división de las mismas en diferentes clases era claramente ineficiente, y en unos pocos años éstas podían llegar a agotarse. Además, las tablas de rutas de los routers comenzaban a crecer de manera desmesurada, y soluciones como el CIDR no podrían solucionar el problema indefinidamente.

Además, con el desarrollo de Internet y su llegada al gran público, habían surgido nuevas necesidades que debían ser cubiertas si se quería que la red pudiera seguir prestando servicio. Por ejemplo, empezaba a ser necesario garantizar la integridad y confidencialidad de los datos enviados a través de la red, poder ofrecer una calidad de servicio garantizada para determinadas aplicaciones en tiempo real o dar soporte a los, cada vez más frecuentes, usuarios móviles. Todo esto llevo a los diferentes organismos involucrados en el desarrollo de Internet, tanto el IAB como el IESG o la IETF, a plantearse la necesidad de un cambio de base en la arquitectura de la red. Es decir, era necesario redise

Además, con el desarrollo de Internet y su llegada al gran público, habían surgido nuevas necesidades que debían ser cubiertas si se quería que la red pudiera seguir prestando servicio. Por ejemplo, empezaba a ser necesario garantizar la integridad y confidencialidad de los datos enviados a través de la red, poder ofrecer una calidad de servicio garantizada para determinadas aplicaciones en tiempo real o dar soporte a los, cada vez más frecuentes, usuarios móviles.

Todo esto llevo a los diferentes organismos involucrados en el desarrollo de Internet, tanto el IAB como el IESG o la IETF, a plantearse la necesidad de un cambio de base en la arquitectura de la red. Es decir, era necesario rediseñar el protocolo sobre el que estaba basada Internet, el IP. Las diferentes líneas de acción que se abrieron es ese momento convergieron en el diseño de un nuevo protocolo, IPv6, sobre la que se asentaría la Internet del futuro.

Este muevo protocolo IPv6 ha sido diseñado teniendo en cuenta la necesidad de disponer de soluciones de autoconfiguración sencillas en el propio protocolo de Internet, y no necesitar emplear otro protocolo de configuración más que cuando deseemos realizar operaciones complejas. Podemos por tanto distinguir dos tipos de autoconfiguración en IPv6, que veremos a continuación: autoconfiguración sin estado y autoconfiguración con estado.

De todas formas, antes de abordar el funcionamiento de ambos mecanismos conviene repasar brevemente la arquitectura de direcciones de IPv6, pues en gran medida es la que posibilita el disponer de mecanismos sencillos de autoconfiguración y, a la vez, es la que impone la necesidad de modificar los protocolos existentes.

Arquitectura de direcciones IPv6

En IPv6, las direcciones son identificadores de 128 bits para interfaces y conjuntos de interfaces. Distinguimos tres tipos principales de direcciones:

- Unicast: Un identificador de un interfaz. Los datagramas enviados a dicha direccion solamente son recibidos por el interfaz asociado.
- Anycast: Un identificador para un conjunto de interfaces (generalmente en nodos distintos). Un datagrama enviado a una dirección anycast será recibido por uno de los interfaces, el mas "cercano".
- Multicast: Un identificador para un conjunto de interfaces. Un datagrama enviado a una dirección multicas será recibido por todos los interfaces.

Como podemos observar, en IPv6 desaparece el concepto de broadcast. Esta funcion se reemplazará por direcciones multicast especiales (cuyo soporte es obligatorio en las implementaciones del protocolo).

Existen dos tipos de direcciones unicast especiales, de uso local. La primera es la de enlace, que debe estar presente en todos los interfaces. Los paquetes dirigidos a esa direccion solo se propagarán por el enlace, y nuca serán rutados por un router. La segunda, es la sitio, que si puede ser rutada dentro de un mismo dominio, pero nunca hacia la Internet.
Existen, asimismo, direcciones multicas especiales para referirse a todos los interfaces de un nodo, a todos los nodos de un enlace, a todos los routers de un enlace,...

Configuracion con Estado. DHCPv6

Cuando se necesitan soluciones más sofisticadas para la configuración de los equipos o si queremos tener un mayor control sobre las direcciones que tienen nuestros equipos, hemos de emplear el mecanismo de configuración con estado de IPv6. Este no es otro que DHCPv6, es decir, una adpatación al nuevo protocolo de Internet del protocolo de DHCP.
Existen diferencias entre ambos protocolos, motivadas principalmente por los siguientes motivos:

- IPv6 soporta un nuevo modelo y una nueva arquitectura de comunicaciones y configuración automática de direcciones.
  - DHCP se beneficia de estos factores.
- Se espera una evolución de los servicios presentes en la red, por lo que se han añadido algunas funcionalidades para poder soportar estos servicios en un futuro.

Entre las diferencias generadas por estos factores, podemos destacar:

- La existencia de direcciones de enlace permite a un nodo tener una dirección nada más arrancar, por lo que cualquier cliente puede emplear esta dirección como fuente para localizar un servidor o un relay de DHCP en el enlace.
  - La necesidad de mantener compatibilidad con BOOTP desaparece.
- La configuración automática con estado debe coexistir con la que no tiene estado, teniendo que ser capaz de detectar direcciones duplicacadas y manejar los tiempos de vida.
  - IPv6 soporta múltiples direcciones por interfaz.
- Algunas opciones de DHCPv4 dejan de tener sentido en IPv6.
- La posibilidad de poder usar direcciones multicast permite que los relays no tengan porque conocer la direccion exacta del servidor.

Conocedores de estas deficiencias, y aprovechando la definición de una nueva versión del protocolo IP, que se ha dado en llamar IPv6, los cuerpos técnicos de Internet diseñaron una especificación de seguridad a nivel de red, capaz de aportar confidencialidad, autenticación e integridad a las comunicaciones sobre IP; a esta especificación se la conoce formalmente como IP Security o IPSec.

En este contexto es donde surge el artículo que aquí presentamos, el cual pretende, partiendo de la problemática actual asociada a IPv4, realizar un repaso a los aspectos más interesantes que aporta IPv6 haciendo especial hincapié en aquellos relacionados con la seguridad, que como veremos, pueden ser de enorme utilidad para añadir un grado adicional de confianza a los intercambios de información que se producen en algunos escenarios de los sistemas de pago actuales.

[Los problemas del protocolo IPv4]

Diseñado originalmente hace más de 20 años para interconectar el amplio y a su vez heterogéneo conjunto de ordenadores del gobierno de los Estados Unidos, el protocolo IP se ha ido convirtiendo con el paso del tiempo en la base de los sistemas de comunicación de la mayoría de las redes públicas y privadas, lo que ha provocado que tanto sus cualidades, como, sobre todo sus importantes defectos, hayan quedado al descubierto.

El principal defecto viene motivado por la debilidad del sistema de direccionamiento, cuyo método de asignación responde a un esquema basado en el tamaño de las organizaciones, a partir del cual nació el modelo de clases que hoy conocemos; en dicho modelo sólo se da cabida a tres tipos de prefijos de longitud predeterminada (para direcciones unicast), utilizados en cada caso según se trate de una organización grande (clase A), mediana (clase B) o pequeña (clase C).

Este método de asignación de direcciones, mientras Internet se empezaba a desarrollar, se mantenía de manera centralizada por parte del SRI-NIC y sin mostrar ninguna debilidad, pero en el momento en el que la red de redes comenzó a crecer de forma significativa, se empezó a observar con preocupación cómo cada vez quedaban menos y menos direcciones libres, llegándose, incluso, no hace mucho tiempo atrás, a utilizar la expresión "agotamiento de las direcciones IP".

Otro problema importante, está relacionado con el hecho de no diferenciar entre distintos flujos de comunicación, asociando así la misma importancia a un tráfico de relleno, como las news, que a una secuencia de paquetes asociada con una videoconferencia, para la

cual la pérdida de un cierto número de datagramas puede alterar, o incluso imposibilitar, la interpretación de la información trasmitida.

La última de las deficiencias, y quizás la de mayor interés para el lector de este artículo, viene motivada por el hecho de ser un medio de comunicación inseguro, lo cual es consecuencia directa del carácter puramente académico de sus primeros años de andadura, que relegó a un segundo plano un aspecto como éste, que hoy en día nos parece fundamental; esta situación se mantuvo así hasta que empezaron a producirse los primeros ataques globales que dieron lugar a notables esfuerzos en la incorporación de seguridad a las aplicaciones existentes, que no a niveles más bajos, como el propio nivel de red.

Para remediar estos problemas, los cuerpos técnicos de Internet impulsaron un debate conocido como IP Next Generation (IPng), que culminó con la especificación de un nuevo protocolo IP, sucesor del actual IPv4, y conocido formalmente como

IPv6, la base de un nivel de seguridad adicional para sistemas de Comercio Electrónico

IP versión 6, o simplemente, IPv6.

[Las características principales de IPv6]

La primera característica que se suele destacar de IPv6 es el mayor tamaño de las direcciones (128 bits frente a los 32 bits de IPv4) que combinado con su nueva estructura basada en la naturaleza de la comunidad a la que va a servir, permite añadir flexibilidad y dinamismo a este protocolo. En este sentido destacar también la incorporación de un nuevo tipo de direcciones, conocidas como anycast, que identifican a un conjunto de interfaces de forma que un paquete enviado a una dirección de este tipo, será entregado a uno de los componentes de ese conjunto, normalmente a aquel más cercano al host origen.

Otro aspecto que ha cambiado de forma significativa en IPv6, es el formato de la cabecera que utiliza este protocolo. Una representación de ambas cabeceras se puede observar en las figuras 1 y 2, de las cuales se puede deducir ya de forma visual que la cabecera IPv6 está considerablemente simplificada en lo que a estructura se refiere, (aunque no así en tamaño, debido a que las direcciones son ahora cuatro veces más grandes), y que mientras la cabecera IPv4 tiene una longitud variable, la correspondiente en IPv6 tiene una longitud

fija de 40 bytes, lo cual permite un procesamiento más eficiente por parte de los routers.

En esta cabecera se han introducido dos campos, conocidos como prioridad (prior.) y etiqueta de flujo, que permiten diferenciar a nivel IP, secuencias de datagramas con naturaleza distinta. Para ello se ha definido un nuevo concepto de flujo, que puede ser visto como un intento de unir la flexibilidad que nos aporta una red basada en paquetes y las garantías que nos ofrece una red basada en circuitos virtuales. Se trata de un identificador que referencia a una secuencia de paquetes enviada desde una fuente a un destino, y para la cual se requiere un manejo especial por parte de los routers que intervienen en la comunicación.

Dicho manejo especial debe de ser indicado de alguna manera a los routers, mediante protocolos de control, como por ejemplo el protocolo de reserva de recursos (RSVP), o por información introducida en el mismo paquete (en alguna cabecera definida con tal propósito); la información relacionada con ese manejo especial es almacenada por los routers en una tabla hash a la cual acceden cuando les llega un paquete con un campo de etiqueta de flujo con un valor distinto de cero, manteniendo de esta forma un contexto de los flujos actualmente en tránsito, dando lugar, por lo tanto, a redes más rápidas y fiables para todos, algo bastante difícil de conseguir con IPv4.

del nivel de aplicación. Estas cabeceras son opcionales y constituyen uno de los elementos de interés del nuevo protocolo, siendo utilizadas como soporte para introducir información relacionada con seguridad, fragmentación del host origen, enrutamiento fuente, gestión de red y cualquier otra nueva funcionalidad que nos pueda interesar en el futuro.

Por último destacar, junto con los aspectos de seguridad que serán tratados en profundidad en el siguiente apartado, la posibilidad de realizar autoconfiguración de equipos, según la cual un ordenador puede descubrir y registrar aquellos parámetros que necesita para conectarse a la red; este mecanismo posibilita también la realización de tareas de mantenimiento y gestión de la red, permitiendo que un

equipo pueda cambiar, por ejemplo, de dirección de forma dinámica si el proveedor de acceso a Internet cambia.

[El estándar de seguridad a nivel IP: IPSec]

Uno de los requisitos que se estableció como básico en el diseño del nuevo protocolo IPv6, fue la incorporación de mecanismos que fueran capaces de dotar de seguridad a las comunicaciones a nivel de red. Después de muchas propuestas y revisiones se llegó a la definición de un protocolo, conocido como IPSec (acrónimo de IP Security) que cumplía los requisitos establecidos.

Considerado como obligatorio en IPv6 y recomendable en IPv4, es independiente de los algoritmos criptográficos utilizados (pudiendo hacer uso de otros nuevos según se vayan diseñando e implementando) y no afecta a las redes y hosts que no lo soportan; ofrece integridad, autenticación de origen, confidencialidad y protección anti-reenvío, valiéndose para ello de la cabecera de autenticación AH (Authentication Header) y de la cabecera de encapsulado seguro de datos ESP (Encapsulation Security Payload).

Cada cabecera soporta dos modos de utilización: modo transporte y modo túnel. En el primer caso se ofrece una protección tanto a los protocolos de nivel superior como a los campos de la cabecera del datagrama IP que no cambian de valor en su camino desde el origen hacia el destino; el modo túnel por su parte, aporta protección total a todo el paquete (incluida la cabecera completa) mediante el encapsulado de éste en un nuevo datagrama. Dependiendo del tipo de información a proteger (mayor protección en el modo túnel) y de la velocidad necesaria (mayor velocidad de procesamiento en el modo transporte) se hará uso de una opción u otra.

Destacar también que ambas cabeceras se basan en un nuevo concepto introducido por IPSec: la asociación de seguridad (Security Association o SA) que especifica una conexión lógica unidireccional entre dos equipos que soportan IPSec, definiendo los servicios de seguridad que serán aportados (utilizando AH o ESP) al tráfico que pase a través de ella.

Entrando un poco más en detalle, la cabecera de autenticación (AH) provee integridad, autenticación de origen y protección anti-reenvío. La autenticación se proporciona para la mayor parte posible de la cabecera IP (todos los campos excepto aquellos que cambian durante el camino del origen al destino) y para los datos de nivel superior. Por su parte la cabecera de encapsulado seguro de datos (ESP) provee el mismo conjunto de servicios que AH añadiendo la confidencialidad.

En otro orden de cosas, y con el objetivo en mente de aportarle al lector una visión completa de la seguridad a nivel de red, destacar que para establecer una conexión segura entre dos entidades se necesita información criptográfica válida, es decir, negociada de forma segura tras una fase previa de autenticación. Para poder realizar esta negociación, el nivel de red es claramente insuficiente y se tiene que recurrir a la utilización de mecanismos de nivel superior, como los protocolos de intercambio de claves. Photuris, SKIP e IKE son las propuestas mas reseñables, siendo esta última, IKE, la que se está convirtiendo, por parte de la comunidad Internet como el estándar de facto.

IPv6, la base de un nivel de seguridad adicional para sistemas de Comercio Electrónico

AH, ESP e IKE (como protocolo de intercambio de claves) se define un entorno de seguridad a nivel de red, caracterizado, frente a otras propuestas a nivel de aplicación, por la transparencia que aporta al usuario final, que cuenta con comunicaciones seguras sin necesidad de conocer claves secretas ni tener conocimientos previos de seguridad.

[La seguridad en el nivel de red aplicada al comercio electrónico]

Los sistemas de comercio electrónico ofrecen a las empresas la posibilidad de mejorar de forma significativa sus oportunidades de negocio y el rendimiento de sus servicios de promoción y venta de productos. Conocedores de esta realidad cada vez más organismos privados están empezando a unirse a esta nueva tendencia tecnológica, montando para ello soluciones software que implementan sistemas de venta en Internet basadas en el estándar SET, que les permiten ofertar sus productos a un número cada vez mayor de compradores.

Dichas soluciones software son capaces de dotar de servicios básicos de seguridad en el escenario de pagos (servicios definidos y aportados por SET), pero no contemplan la necesidad de un nivel mínimo de seguridad para otros escenarios como la administración remota de comercios, la negociación entre cliente y proveedor, etc. En este sentido pensemos en la posibilidad de que los datos introducidos desde casa por un comerciante (o grupo de comerciantes) no coincidan con los reflejados en su Base de Datos de productos ofertados, o que, estemos recibiendo como clientes ofertas del proveedor manipuladas por terceros (que no se ajusten a la realidad).

Estas deficiencias que acabamos de plantear, no son sino una pequeña muestra de algunas situaciones en las cuales los sistemas de comercio electrónico podrían producir (fuera del entorno de pagos, claro está) insatisfacción entre los interlocutores involucrados (clientes y proveedores sobre todo).

Para solventar algunos de estos problemas, como por ejemplo, los relacionados con la administración remota y segura de comercios (que lleva asociada normalmente el intercambio de grandes cantidades de información) una buena opción (incluso mejor que la de los certificados digitales) sería el desarrollo de una infraestructura de seguridad a nivel de red (actualmente sobre IPv4 y en no mucho tiempo sobre IPv6) basada en la utilización de IPSec e IKE, que tal y como comentábamos en apartados anteriores, se están erigiendo como solución de facto sobre sistemas de comunicación IP. La utilización de este tipo de infraestructuras de seguridad, permitiría dotar de confidencialidad e integridad a las comunicaciones, propiedades éstas que son de enorme interés, sobre todo la integridad, para cualquier intercambio de información.

También es importante reseñar que la consecución de estos objetivos viene caracterizada por una trasparencia para el usuario final, y cualquier aplicación que éste tenga en su ordenador, ya que los sistemas IPSec/IKE formarían parte de las pilas TCP/IP asociadas a la distribución de los propios sistemas operativos.

[Conclusiones]

Las deficiencias manifiestas del protocolo IP en su versión 4, impiden en cierta medida el desarrollo de nuevas tecnologías que impulsen a Internet como un sistema real de comercio e intercambio de información electrónica. Pero estas deficiencias tocan a su fin como consecuencia de la definición, y según todos los autores, pronta implantación de la nueva versión del protocolo IP, conocida formalmente como IPv6. Entre sus características más sobresalientes cuenta con direcciones de 128 bits, mecanismos de priorización de flujos de información de distinta naturaleza, sistemas de autoconfiguración y mecanismos de seguridad (aportada por el protocolo IPSec).

Este protocolo, en combinación con el estándar de facto dentro de los sistemas de intercambio de claves, IKE, da lugar a una plataforma de seguridad de enorme interés, debido a que aportan confidencialidad, autenticación e integridad de forma

El IP versión 6 (IPv6) es la nueva versión del Protocolo Internet, diseñado como el sucesor para el IP versión 4 (IPv4) [RFC-791]. Los cambios del IPv4 al IPv6 recaen principalmente en las siguientes

categorías:

- Capacidades de Direccionamiento Extendida

El IPv6 incrementa el tamaño de dirección IP de 32 bits a 128 bits, para dar soporte a más niveles de direccionamiento jerárquico, un número mucho mayor de nodos direccionables, y una autoconfiguración más simple de direcciones. La escalabilidad del enrutamiento multienvío se mejora agregando un campo "ámbito" a las direcciones multienvío. Y se define un nuevo tipo de dirección llamada "dirección envío a uno de", usado para enviar un paquete a cualquiera de un grupo de nodos.

- Simplificación del Formato de Cabecera

Algunos campos de la cabecera IPv4 se han sacado o se han hecho opcional, para reducir el costo del caso común de proceso de tratamiento de paquete y para limitar el costo del ancho de banda, de la cabecera IPv6.

o Soporte Mejorado para las Extensiones y Opciones

Los cambios en la manera en que se codifican las opciones de la cabecera IP permiten un reenvío más eficiente, límites menos rigurosos en la longitud de opciones, y mayor flexibilidad para introducir nuevas opciones en el futuro.

o Capacidad de Etiquetado de Flujo

Una nueva capacidad se agrega para permitir el etiquetado de paquetes que pertenecen a "flujos" de tráfico particulares para lo cuál el remitente solicita tratamiento especial, como la calidad de servicio no estándar o el servicio en "tiempo real".

o Capacidades de Autenticación y Privacidad

Extensiones para utilizar autenticación, integridad de los datos, y (opcional) confidencialidad de los datos, se especifican para el IPv6.

Este documento especifica la cabecera IPv6 básica y las cabeceras de extensión IPv6 y las opciones inicialmente definidas. Aborda también

cuestiones de tamaño del paquete, las semánticas de las etiquetas de flujo y las clases de tráfico, y los efectos del IPv6 en protocolos de capa superior. Los formatos y semánticas de las direcciones IPv6 son especificadas separadamente en [ADDRARCH]. La versión IPv6 del ICMP, que a todas las implementaciones IPv6 se exige incluir, es especificada en [ICMPv6].

2. Terminología

nodo - un dispositivo que implementa el IPv6.

enrutador - un nodo que reenvía paquetes IPv6 no explícitamente destinados hacia sí mismo. [Ver Nota abajo].

host - cualquier nodo que no es un enrutador. [Ver Nota abajo].

capa superior - una capa de protocolo inmediatamente encima del IPv6. Ejemplos son los protocolos transporte tal como el TCP y el UDP, protocolos control tal como el ICMP, protocolos enrutamiento tal como el OSPF, y protocolos internet o de capa inferior que están siendo "tunelizados" sobre (es decir, encapsulados dentro) IPv6 tal como el IPX, el AppleTalk, o

el mismo IPv6.

enlace - una facilidad de comunicación o medio sobre el cual los nodos pueden comunicarse en la capa de enlace, es decir, la capa inmediatamente debajo del IPv6. Ejemplos son las Ethernets (simples o de puentes); enlaces PPP; X.25, Frame Relay, o redes ATM; y "túneles" de capa internet (o superior), tal como los túneles sobre IPv4 o sobre el mismo IPv6.

vecinos - nodos conectados al mismo enlace.

interface - lo que acopla un nodo a un enlace.

dirección - un identificador de capa IPv6 para una interface o un conjunto de interfaces.

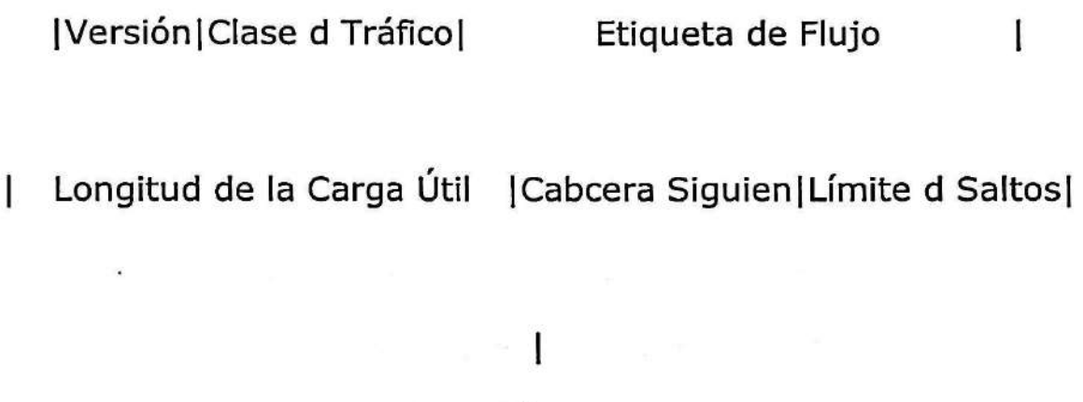
paquete - una cabecera IPv6 más carga útil.

MTU de enlace - la unidad de transmisión máxima, es decir, el tamaño del paquete máximo en octetos, que puede transportarse sobre un enlace.

MTU de ruta - la MTU de enlace mínima de todos los enlaces dentro de una ruta entre un nodo origen y un nodo destino.

Nota: es posible, aunque inusual, para un dispositivo con interfaces múltiples ser configurado para reenviar paquetes no autodestinados que llegan desde algún conjunto (menos que todas) de sus interfaces, y para descartar paquetes no autodestinados que llegan desde sus otras interfaces. Un dispositivo semejante debe cumplir con los requisitos de protocolo para enrutadores al recibir paquetes de, e interactuar con vecinos sobre, las interfaces anteriores (reenviantes). Debe cumplir con los requisitos de protocolo para hosts la recibir paquetes de, e interactuar con vecinos sobre, las interfaces posteriores (no reenviantes).

3. Formato de la Cabecera IPv6



Versión — Número = 6 de versión del Protocolo Internet de 4 bits.

Clase de Tráfico — Campo clase de tráfico de 8 bits. Ver la sección 7.

Etiqueta de Flujo — Etiqueta de flujo de 20 bits. Ver la sección 6.

Longitud de la Carga Útil Entero sin signo de 16 bits. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos. (Notar que cualesquiera de las cabeceras de extensión [sección 4] presente es considerada parte de la carga útil, es decir, incluida en el conteo de la longitud).

Cabecera Siguiente Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].

Límite de Saltos Entero sin signo de 8 bits. Decrementado en 1 por cada nodo que reenvía el paquete. Se descarta el paquete si el Límite de Saltos es decrementado hasta cero.

Dirección Origen Dirección de 128 bits del originador del paquete. Ver la [ADDRARCH].

Dirección Destino Dirección de 128 bits del recipiente pretendido del paquete (posiblemente no el último recipiente, si está presente una cabecera Enrutamiento). Ver la [ADDRARCH] y la sección 4.4.

4. Cabeceras de Extensión IPv6

En el IPv6, la información de capa internet opcional se codifica en cabeceras separadas que se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior dentro de un paquete. Hay un número pequeño de tales cabeceras de extensión, cada una identificada por un valor de Cabecera Siguiente distinto. Según lo ilustrado en estos ejemplos, un paquete IPv6 puede llevar cero, una, o más cabeceras de

extensión, cada una identificada por el campo Cabecera Siguiente de la cabecera precedente:

CABEZERA DE EMRRUTAMIENTO

Con una excepción, las cabeceras de extensión no son examinadas ni procesadas por ningún nodo a lo largo de la ruta de entrega de un paquete, hasta que el paquete alcance el nodo (o cada uno del conjunto de nodos, en el caso de multienvío) identificado en el campo Dirección Destino de la cabecera IPv6. Allí, el demultiplexaje normal en el campo Cabecera Siguiente de la cabecera IPv6 invoca el módulo para procesar la primera cabecera de extensión, o la cabecera de capa superior si no hay ninguna cabecera de extensión presente. El contenido y la semántica de cada cabecera de extensión determinan si se procede o no a la cabecera siguiente. Por lo tanto, las cabeceras de extensión se deben procesar estrictamente en el orden que aparecen en el paquete; un receptor no debe, por ejemplo, examinar a través de un paquete buscando un tipo en particular de cabecera de extensión y procesar esa cabecera antes de procesar todas las precedentes.

La excepción mencionada en el párrafo precedente es la cabecera Opciones de Salto a Salto, la cual lleva información que debe ser

examinada y procesada por cada nodo a lo largo de la ruta de entrega

de un paquete, incluyendo los nodos de origen y de destino. La

cabecera Opciones de Salto a Salto, cuando está presente, debe seguir

inmediatamente a la cabecera IPv6. Su presencia es indicada por el

valor cero en el campo Cabecera Siguiente de la cabecera IPv6.

Si, como resultado de procesar una cabecera, un nodo necesita

proceder a la cabecera siguiente pero el valor Cabecera Siguiente en

la cabecera actual es desconocido por el nodo, debe descartar el

paquete y enviar un mensaje ICMP de Problema de Parámetro al origen

del paquete, con un valor Código ICMP de 1 ("encontrado tipo de

Cabecera Siguiente desconocido") y el campo Puntero ICMP conteniendo

el desplazamiento del valor desconocido dentro del paquete original.

La misma acción se debería tomar si un nodo encuentra un valor

Cabecera Siguiente de cero en cualquier cabecera con excepción de una

cabecera IPv6.

Cada cabecera de extensión es un entero múltiplo de 8 octetos de

largo, para conservar la alineación de 8 octetos para las cabeceras

subsiguientes. Los campos Multiocteto dentro de cada cabecera de

extensión se alinean en sus límites naturales, es decir, los campos

de ancho de n octetos son colocados en un entero múltiplo de n

octetos desde el inicio de la cabecera, para n = 1, 2, 4, o 8.

Una implementación completa del IPv6 comprende la implementación de

las siguientes cabeceras de extensión:

Opciones de Salto a Salto

Enrutamiento (Tipo 0)

Fragmento

Opciones de Destino

Autenticación

Seguridad del Encapsulado de la Carga Útil

Las primeras cuatro están especificadas en este documento; las

últimas dos están especificadas en la [RFC-2402] y la [RFC-2406],

respectivamente.

4.1 Orden de las Cabeceras de Extensión

Cuando más de una cabecera de extensión se usa en un mismo paquete,

se recomienda que esas cabeceras aparezcan en el siguiente orden:

Cabecera IPv6

Cabecera Opciones de Salto a Salto

Cabecera Opciones de Destino (nota 1)

Cabecera Enrutamiento

Cabecera Fragmento

Cabecera Autenticación (nota 2)

Cabecera Seguridad del Encapsulado de la Carga Útil (nota 2)

Cabecera Opciones de Destino (nota 3)

Cabecera de Capa Superior

nota 1: para las opciones a ser procesadas por el primer destino que aparece en el campo Dirección Destino IPv6 más los destinos subsiguientes listados en la Cabecera Enrutamiento.

nota 2: recomendaciones adicionales con respecto al orden relativo de las cabeceras Autenticación y Seguridad del Encapsulado de la Carga Útil se dan en la [RFC-2406].

nota 3: para las opciones a ser procesadas solo por el destino final del paquete.

Cada cabecera de extensión debe ocurrir solamente una vez, a excepción de la cabecera Opciones de Destino la cual debe de ocurrir a lo sumo dos veces (una vez antes de una cabecera Enrutamiento y la otra vez antes de una cabecera de capa superior).

Si la cabecera de capa superior es otra cabecera IPv6 (en el caso de que el IPv6 sea tunelizado o encapsulado en el IPv6), puede ser seguida por sus propias cabeceras de extensión, las cuales están separadamente sujetas a las mismas recomendaciones de orden.

Siempre y cuando se definan otras cabeceras de extensión, sus restricciones de orden concerniente a las cabeceras arriba listadas deben ser especificadas.

Los nodos IPv6 deben aceptar e intentar procesar cabeceras de extensión en cualquier orden y cualquier número de veces que ocurran en un mismo paquete, a excepción de la cabecera Opciones de Salto a Salto la cual está restringida a aparecer sólo inmediatamente después de una cabecera IPv6. No obstante, se aconseja fuertemente que los

originadores de paquetes IPv6 se apeguen al orden recomendado arriba

hasta y a menos que especificaciones subsiguientes corrijan esa recomendación.

4.2 Opciones

Dos de las cabeceras de extensión actualmente definidas -- la cabecera Opciones de Salto a Salto y la cabecera Opciones de Destino -- llevan un número variable de "opciones" codificadas tipo-longitud-valor (TLV), de la siguiente forma:

Tipo de Opción	Identificador de 8 bits del tipo de opción.
Lon Datos Opc	Entero sin signo de 8 bits. Longitud del campo Datos de la Opción de esta opción, en octetos.
Datos de la Opción	Campo de longitud variable. Datos específicos del Tipo de Opción.

La secuencia de opciones dentro de una cabecera se deben procesar

estrictamente en el orden que aparecen en la cabecera; un receptor no

debe, por ejemplo, examinar a través de una cabecera buscando un tipo

en particular de opción y procesar esa opción antes de procesar todas las precedentes.

Los identificadores Tipo de Opción se codifican internamente tales que sus 2 bits de más alto orden especifican la acción que se debe tomar si el nodo IPv6 en proceso no reconoce el Tipo de Opción:

00 - no tomar en cuenta esta opción y continuar procesando la cabecera.

01 - descartar el paquete.

10 - descartar el paquete y, sin tener en cuenta si o no la Dirección Destino del paquete fue una dirección multienvío, enviar un mensaje ICMP Problema de Parámetro, Código 2, a la Dirección Origen del paquete señalando el Tipo de Opción desconocido.

11 - descartar el paquete y, solo si la Dirección Destino del paquete no fue una dirección multienvío, enviar un mensaje ICMP Problema de Parámetro, Código 2, a la Dirección Origen

del paquete señalando el Tipo de Opción desconocido.

El tercer bit de más alto orden del Tipo de Opción especifica si o no los Datos de la Opción de esa opción pueden modificar el enrutado hacia el destino final del paquete. Cuando una cabecera Autenticación

está presente en el paquete, para cualquier opción cuyos datos pueden

modificar el enrutado, su campo entero Datos de la Opción se debe tratar como octetos de valor cero cuando se calcula o verifica el valor de autenticidad del paquete.

0 - los Datos de la Opción no modifican el enrutado.

1 - los Datos de la Opción pueden modificar el enrutado.

Los tres bits de alto orden descritos arriba están para ser tratados como parte del Tipo de Opción, no independientemente del Tipo de Opción. Es decir, una opción en particular se identifica por un Tipo de Opción de 8 bits completo, no sólo por los 5 bits de bajo orden de un Tipo de Opción.

El mismo espacio de enumeración del Tipo de Opción se usa tanto para

la cabecera Opciones de Salto a Salto como para la cabecera Opciones

de Destino. Sin embargo, la especificación de una opción en particular puede restringir su uso a solamente una de esas dos cabeceras.

Las opciones individuales pueden tener requisitos específicos de alineación, para asegurar que los valores multiocteto dentro de los campos Datos de la Opción caigan en límites naturales. El requisito de alineación de una opción se especifica usando la notación xn+y, lo que significa que el Tipo de Opción debe aparecer en un entero múltiplo de x octetos desde el inicio de la cabecera, más y octetos. Por ejemplo:

2n significa cualquier desplazamiento de 2 octetos a partir del comienzo de la cabecera.

8n+2 significa cualquier desplazamiento de 8 octetos a partir del comienzo de la cabecera, más 2 octetos.

Hay dos opciones de relleno las cuales se usan cuando es necesario alinear opciones subsiguientes y rellenar la cabecera contenedora a una longitud múltiplo de 8 octetos. Estas opciones de relleno deben ser reconocidas por todas las implementaciones IPv6:

Opción Pad1 (requisito de alineación: ninguno)

NOTA! el formato de la opción Pad1 es un caso especial -- no tiene los campos longitud y valor.

La opción Pad1 se usa para insertar un octeto de relleno dentro del área de Opciones de una cabecera. Si se requiere más de un octeto de relleno, la opción PadN, descrita a continuación, se debería usar, en lugar de múltiples opciones Pad1.

Opción PadN (requisito de alineación: ninguno)

La opción PadN se usa para insertar dos o más octetos de relleno dentro del área de Opciones de una cabecera. Para N octetos de relleno, el campo Lon Datos Opc contiene el valor N-2, y el campo Datos de la Opción consiste en N-2 octetos de valor cero.

El Apéndice B contiene pautas de formateo para diseñar Opciones nuevas.

4.3 Cabecera Opciones de Salto a Salto

La cabecera Opciones de Salto a Salto se usa para llevar información opcional que debe ser examinada por cada nodo a lo largo de la ruta

de entrega de un paquete. La cabecera Opciones de Salto a Salto se identifica por un valor Cabecera Siguiente de 0 en la cabecera IPv6, y tiene el siguiente formato:

Opciones

Cabecera Siguiente Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Opciones de Salto a Salto. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].

Lon Cab Ext Entero sin signo de 8 bits. Longitud de la cabecera Opciones de Salto a Salto en unidades de 8 octetos, no incluye los primeros 8 octetos.

Opciones Campo de longitud variable, de longitud tal que la cabecera Opciones de Salto a Salto completa es un entero múltiplo de 8 octetos de largo. Contiene una o más opciones codificadas TLV,

como se describe en la sección 4.2.

Las únicas opciones de salto a salto definidas en este documento son las opciones Pad1 y PadN especificadas en la sección 4.2.

4.4 Cabecera Enrutamiento

La cabecera Enrutamiento es utilizada por un origen IPv6 para listar uno o más nodos intermedio a ser "visitados" en el camino hacia el destino de un paquete. Esta función es muy similar a las opciones Origen Impreciso y Registro de Ruta del IPv4. La cabecera Enrutamiento se identifica por una Cabecera Siguiente de valor 43 en la cabecera inmediatamente precedente, y tiene el siguiente formato:

Cabecera Siguiente	Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Enrutamiento. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].
Lon Cab Ext	Entero sin signo de 8 bits. Longitud de la cabecera Enrutamiento en unidades de 8 octetos, no incluye los primeros 8

octetos.

Tipo de Enrutamiento Identificador de 8 bits de una variante en particular de cabecera Enrutamiento.

Segmentos Dejados Entero sin signo de 8 bits. Número de segmentos de ruta restantes, es decir, número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el destino final.

Datos específicos del tipo Campo de longitud variable, de formato determinado por el Tipo de Enrutamiento, y de longitud tal que la cabecera Enrutamiento completa es un entero múltiplo de 8 octetos de largo.

Si, al procesar un paquete recibido, un nodo encuentra una cabecera Enrutamiento con un valor Tipo de Enrutamiento desconocido, el comportamiento requerido del nodo depende del valor del campo Segmentos Dejados, como sigue:

Si Segmentos Dejados es cero, el nodo debe ignorar la cabecera

Enrutamiento y proceder a procesar la siguiente cabecera en el paquete, cuyo tipo se identifica por el campo Cabecera Siguiente en la cabecera Enrutamiento.

Si Segmentos Dejados no es cero, el nodo debe descartar el paquete y enviar un mensaje ICMP Problema de Parámetro, Código 0, a la Dirección Origen del paquete, apuntando al Tipo de Enrutamiento desconocido.

Si, después de procesar una cabecera Enrutamiento de un paquete recibido, un nodo intermedio determina que el paquete será remitido hacia un enlace cuya MTU de enlace es menor que el tamaño del paquete, el nodo debe descartar el paquete y enviar un mensaje ICMP

Paquete Demasiado Grande a la Dirección Origen del paquete.

La cabecera Enrutamiento de Tipo 0 tiene el siguiente formato:

Reservado

Cabecera Siguiente Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Enrutamiento. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].

Lon Cab Ext Entero sin signo de 8 bits. Longitud de la cabecera Enrutamiento en unidades de 8 octetos, sin incluir los primeros 8 octetos. Para la cabecera Enrutamiento de Tipo 0, Lon Cab Ext es igual a dos veces el número de direcciones en la cabecera.

Tipo de Enrutamiento 0.

Segmentos Dejados Entero sin signo de 8 bits. Número de segmentos de ruta restantes, es decir, número de nodos intermedio explícitamente listados aún a ser visitados antes de alcanzar el

destino final.

Reservado Campo reservado de 32 bits. Inicializado a cero para la transmisión; ignorado en la recepción.

Dirección[1..n] Vector de direcciones de 128 bits, numerados desde 1 hasta n.

Las direcciones multienvío no deben aparecer en una cabecera Enrutamiento de Tipo 0, o en el campo Dirección Destino IPv6 de un paquete que lleva una cabecera Enrutamiento de Tipo 0.

Una cabecera Enrutamiento no se examina o procesa hasta que alcance

el nodo identificado en el campo Dirección Destino de la cabecera IPv6. En ese nodo, al despachar el campo Cabecera Siguiente de la cabecera inmediatamente precedente ocasiona que el módulo cabecera

Enrutamiento sea invocado, el cual, en el caso de Enrutamiento Tipo 0, lleva a cabo el siguiente algoritmo:

si Segmentos Dejados = 0 {

proceder a procesar la cabecera siguiente en el paquete, cuyo tipo se identifica por el campo Cabecera Siguiente en la cabecera Enrutamiento

}

sino si Lon Cab Ext es impar {

enviar un mensaje ICMP Problema de Parámetro, Código 0, a la Dirección Origen, apuntando al campo Lon Cab Ext, y descartar el paquete

}

sino {

calcular n, el número de direcciones en la cabecera Enrutamiento, al dividir Lon Cab Ext por 2

si Segmentos Dejados es mayor que n {

enviar un mensaje ICMP Problema de Parámetro, Código 0, a la Dirección de Origen, apuntando al campo Segmentos Dejados, y descartar el paquete

}

sino {

decrementar Segmentos Dejados en 1;

calcular i, el índice de la dirección siguiente a ser visitado en el vector de dirección, substrayendo Segmentos Dejados de n

si la Dirección [i] o la Dirección Destino IPv6 es multienvío {

descartar el paquete

}

sino {

intercambiar la Dirección Destino IPv6 y la Dirección [i]

si el Límite de Saltos es menor que o iguala a 1 {

enviar un mensaje ICMP Tiempo Excedido -- Límite de Saltos Excedido en Transito a la Dirección Origen y

descartar el paquete

}

sino {

decrementar el Límite de Saltos en 1

resometer el paquete al módulo IPv6 para la transmisión

hacia el nuevo destino

}

}

}

}

Como un ejemplo de los efectos del algoritmo de arriba, considerar el caso de un nodo origen S que envía un paquete al nodo de destino D, usando una cabecera Enrutamiento para causar que el paquete sea enrutado vía los nodos intermedio I1, I2, e I3. Los valores de los campos pertinentes de la cabecera IPv6 y de la cabecera Enrutamiento

en cada segmento de la ruta de entrega serían como sigue:

Conforme el paquete viaja de S a I1:

Dirección de Origen = S Lon Cab Ext = 6

Dirección de Destino = I1 Segmentos Dejados = 3

Dirección[1] = I2

Dirección[2] = I3

Dirección[3] = D

Conforme el paquete viaja de I1 a I2:

Dirección de Origen = S Lon Cab Ext = 6

Dirección de Destino = I2 Segmentos Dejados = 2

Dirección[1] = I1

Dirección[2] = I3

Dirección[3] = D

Conforme el paquete viaja de I2 a I3:

Dirección de Origen = S Lon Cab Ext = 6

Dirección de Destino = I3 Segmentos Dejados = 1

Dirección[1] = I1

Dirección[2] = I2

Dirección[3] = D

Conforme el paquete viaja de I3 a D:

Dirección de Origen = S Lon Cab Ext = 6

Dirección de Destino = D Segmentos Dejados = 0

Dirección[1] = I1

Dirección[2] = I2

Dirección[3] = I3

4.5 Cabecera Fragmento

La cabecera Fragmento es utilizada por un origen IPv6 para enviar un paquete más grande de lo que cabría en la MTU de la ruta hacia su destino. (Nota: a diferencia del IPv4, la fragmentación en el IPv6 sólo se lleva a cabo por los nodos origen, no por los enrutadores a lo largo de la ruta de entrega de un paquete -- ver sección 5.) La cabecera Fragmento se identifica por un valor Cabecera Siguiente de 44 en la cabecera inmediatamente precedente, y tiene el siguiente formato:

Identificación

Cabecera Siguiente Selector de 8 bits. Identifica el tipo

de cabecera inicial de la Parte Fragmentable del paquete original (definido abajo). Usa los mismos valores que el campo Protocolo del IPv4 [EL RFC-1700 ET SEQ.].

Reservado — Campo reservado de 8 bits. Inicializado a cero para la transmisión; ignorado en la recepción.

Desplazamiento del Fragmento — Entero sin signo de 13 bits. El desplazamiento, en unidades de 8 octetos, de los datos que siguen a esta cabecera, relativo al comienzo de la Parte Fragmentable del paquete original.

Res — Campo reservado de 2 bits. Inicializado a cero para la transmisión; ignorado en la recepción.

Bandera M — 1 = más fragmentos; 0 = último fragmento.

Identificación	32 bits. Ver descripción abajo.

Para enviar un paquete que es demasiado grande para caber en la MTU de la ruta hacia su destino, un nodo origen puede dividir el paquete en fragmentos y enviar cada fragmento como un paquete separado, para ser reensamblado en el receptor.

Por cada paquete que será fragmentado, el nodo origen genera un valor Identificación. La Identificación debe ser diferente que el de cualquier otro paquete fragmentado enviado recientemente* con la misma Dirección Origen y Dirección Destino. Si una cabecera Enrutamiento está presente, la Dirección Destino de interés es la del destino final.

* "recientemente" significa dentro del máximo tiempo de vida probable de un paquete, incluyendo el tiempo de tránsito del origen hacia el destino y el tiempo gastado esperando el reensemblaje con otros fragmentos del mismo paquete. Sin embargo, no se requiere que un nodo origen conozca el máximo tiempo de vida de un paquete. Más bien, se asume que el requisito puede encontrarse manteniendo el valor Identificación como un simple, contador "envoltura alrededor", de 32 bits, incrementado cada vez que un paquete debe fragmentarse. Es una

opción de implementación si para mantener a un solo contador para el nodo o contadores múltiples, por ejemplo, uno para cada una de las posibles direcciones origen del nodo, o uno para cada combinación (dirección origen, dirección destino) activa.

El paquete inicial, grande, no fragmentado es referido como el "paquete original", y se considera que consiste en dos partes, tal como se ilustra:

paquete original:

La Parte No Fragmentable consiste en la cabecera IPv6 más cualesquiera de las cabeceras de extensión que debe procesarse por nodos en camino hacia el destino, es decir, todas las cabeceras e incluso la cabecera Enrutamiento si esta presente, sino la cabecera Opciones de Salto a Salto si esta presente, sino ninguna de las cabeceras de extensión.

La Parte Fragmentable consiste en el resto del paquete, es decir, cualquiera de las cabeceras de extensión que necesita que sólo se procese por el nodo(s) destino final, más la cabecera de capa superior y los datos.

La Parte Fragmentable del paquete original es dividida en fragmentos,

cada uno, excepto posiblemente el último ("el de la extrema derecha"), siendo un entero múltiplo de 8 octetos de largo. Los fragmentos se transmiten en "paquetes fragmento" separados tal como

se ilustra:

Cada paquete fragmento está compuesto de:

(1) La Parte No Fragmentable del paquete original, con la Longitud de la Carga Útil de la cabecera IPv6 original cambiada para contener la longitud de tan sólo este paquete fragmento (excluyendo la longitud de la propia cabecera IPv6), y el campo Cabecera Siguiente de la última cabecera de la Parte No Fragmentable cambiado a 44.

(2) Una cabecera Fragmento conteniendo:

El valor Siguiente Cabecera que identifica la primera cabecera de la Parte Fragmentable del paquete original.

Un Desplazamiento del Fragmento que contiene el desplazamiento del fragmento, en unidades de 8 octetos, relativo al comienzo de la Parte Fragmentable del paquete original. El Desplazamiento del Fragmento del primer ("el

de la extrema izquierda") fragmento es 0.

Una bandera M de valor 0 si el fragmento es el último

("el de la extrema derecha"), sino una bandera M de valor

El valor Identificación generado para el paquete

original.

(3) El propio fragmento.

Deben escogerse las longitudes de los fragmentos tal que los paquetes

fragmento resultantes quepan dentro de la MTU de la ruta hacia el(los)

destino(s) del paquete.

En el destino, se reensamblan los paquetes fragmento en su forma

original, no fragmentada, tal como se ilustra:

paquete original reensamblado:

Las siguientes reglas gobiernan el reensamblaje:

Un paquete original sólo se reensambla a partir de paquetes fragmento que tienen la misma Dirección Origen, Dirección Destino, e Identificación del Fragmento.

La Parte No Fragmentable del paquete reensamblado consiste en todas las cabeceras, pero sin incluir, la cabecera Fragmento del primer paquete fragmento (es decir, el paquete cuyo Desplazamiento del Fragmento es cero), con los siguiente dos cambios:

El campo Cabecera Siguiente de la última cabecera de la Parte No Fragmentable se obtiene del campo Cabecera Siguiente de la cabecera Fragmento del primer fragmento.

Se calcula la Longitud de la Carga Útil del paquete reensamblado a partir de la longitud de la Parte No Fragmentable y de la longitud y desplazamiento del último fragmento. Por ejemplo, una fórmula para calcular la Longitud de la Carga Útil del paquete original reensamblado es:

LCU.orig = LCU.inicial - LF.inicial - 8 + (8*DF.final) + LF.final

donde

LCU.orig = campo Longitud de la Carga Útil del paquete

reensamblado.

LCU.inicial = campo Longitud de la Carga Útil del primer paquete fragmento.

LF.inicial = longitud del fragmento siguiente a la cabecera Fragmento del primer paquete fragmento

DF.final = campo Desplazamiento del Fragmento de la cabecera Fragmento del último paquete fragmento.

LF.final = longitud del fragmento siguiente a la cabecera Fragmento del último paquete fragmento.

La Parte Fragmentable del paquete reensamblado se construye a partir de los fragmentos siguientes a las cabeceras Fragmento dentro de cada uno de los paquetes fragmento. La longitud de cada fragmento es calculada substrayendo de la Longitud de la Carga Útil del paquete la longitud de las cabeceras entre la cabecera IPv6 y el propio fragmento, su posición relativa en la Parte Fragmentable se calcula a partir de su valor Desplazamiento del Fragmento.

La cabecera Fragmento no está presente en el paquete reensamblado,

final.

Las siguientes condiciones de error pueden originarse al reensamblar paquetes fragmentados:

Si se reciben fragmentos insuficientes para completar el reensamblaje de un paquete dentro de los 60 segundos a partir de la recepción del primer fragmento en llegar de ese paquete, el reensamblaje de ese paquete debe abandonarse y deben descartarse todos los fragmentos que se han recibido para ese paquete. Si el primer fragmento (es decir, el único con un Desplazamiento del Fragmento de cero) se ha recibido, un mensaje ICMP Tiempo Excedido

-- Tiempo Excedido para el Reensamblaje del Fragmento, debe enviarse al origen de ese fragmento.

Si la longitud de un fragmento, tal como se dedujo a partir del campo Longitud de la Carga Útil del paquete fragmento, no es un múltiplo de 8 octetos y la bandera M de ese fragmento es 1, entonces ese fragmento debe descartarse y un mensaje ICMP Problema

de Parámetro, Código 0, debe enviarse al origen del fragmento, apuntando al campo Longitud de la Carga Útil del paquete fragmento.

Si la longitud y el desplazamiento de un fragmento son tales que

la Longitud de la Carga Útil del paquete reensamblado de ese fragmento excedería los 65,535 octetos, entonces ese fragmento debe descartarse y un mensaje ICMP Problema de Parámetro, Código 0, debe enviarse al origen del fragmento, apuntando al campo Desplazamiento del Fragmento del paquete fragmento.

No se espera que las siguientes condiciones ocurran, pero no se consideran errores si lo hacen:

El número y contenido de las cabeceras que preceden a la cabecera Fragmento de fragmentos diferentes del mismo paquete original pueden diferir. Cualesquiera de las cabeceras que estén presentes, precediendo a la cabecera Fragmento en cada paquete fragmento, se procesan cuando los paquetes llegan, previamente a que los fragmentos hagan cola para el reensamblaje. Sólo aquellas cabeceras en el paquete fragmento de Desplazamiento cero se retienen en el paquete reensamblado.

Los valores Cabecera Siguiente en las cabeceras Fragmento de fragmentos diferentes del mismo paquete original pueden diferir.

Sólo el valor del paquete fragmento de Desplazamiento cero se usa para el reensamblaje.

4.6 Cabecera Opciones de Destino

La cabecera Opciones de Destino es usada para llevar información opcional que necesita ser examinada solamente por el(los) nodo(s) destino del paquete. La cabecera Opciones de Destino es identificada por un valor Cabecera Siguiente de 60 en la cabecera inmediatamente precedente, y tiene el siguiente formato:

OPSIONES

Cabecera Siguiente — Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Opciones de Destino. Utiliza los mismos valores que el campo Protocolo del IPv4 [RFC-1700 et seq.].

Lon Cab Ext — Entero sin signo de 8 bits. Longitud de la cabecera Opciones de Destino en unidades de 8 octetos, no incluye los primeros 8 octetos.

Opciones Campo de longitud variable, de longitud tal que la cabecera Opciones de Destino completa es un entero múltiplo de 8 octetos de largo. Contiene uno o más opciones codificadas TLV, tal como se describe en la sección 4.2.

Las únicas opciones de destino definidas en este documento son las opciones Pad1 y PadN especificadas en la sección 4.2.

Notar que hay dos posibles maneras de codificar información de destino opcional en un paquete IPv6: como una opción en la cabecera Opciones de Destino, o como una cabecera de extensión separada. La cabecera Fragmento y la cabecera Autenticación son ejemplos de la más

reciente propuesta. Qué propuesta puede ser usada depende de qué acción es deseada de un nodo destino que no entiende la información opcional:

- Si la acción deseada es que el nodo destino descarte el paquete y, sólo si la Dirección Destino del paquete no es una dirección multienvío, enviar un mensaje ICMP Tipo No reconocido a la Dirección Origen del paquete, luego la información puede ser codificada como una cabecera separada o como una opción en la cabecera Opciones de Destino cuyo Tipo de Opción tiene el valor

11 en sus dos bits de más alto orden. La elección puede depender de factores tales como cual toma menos octetos, o cual rinde mejor alineación o más eficiente análisis.

o Si alguna otra acción es deseada, la información debe ser codificada como una opción en la cabecera Opciones de Destino cuyo Tipo de Opción tiene el valor 00, 01, o 10 en sus dos bits de más alto orden, especificando la acción deseada (ver sección 4.2).

4.7 Cabecera No Hay Siguiente

El valor 59 en el campo Cabecera Siguiente de una cabecera IPv6 o de cualquier cabecera de extensión indica que nada hay siguiendo esa cabecera. Si el campo Longitud de la Carga Útil de la cabecera IPv6 indica la presencia de octetos más allá del final de una cabecera cuyo campo Cabecera Siguiente contiene 59, esos octetos deben ignorarse, y pasarse inalterados si el paquete se reenvía.

5. Cuestiones de Tamaño del Paquete

El IPv6 requiere que cada enlace en la internet tenga una MTU de 1280 octetos o mayor. En cualquier enlace que no pueda llevarse un paquete

de 1280 octetos en una pieza, debe proporcionarse fragmentación y reensamblaje especifico al enlace en una capa debajo del IPv6.

Los Enlaces que tienen una MTU configurable (por ejemplo, enlaces PPP [RFC-1661]) deben configurarse para tener una MTU de por lo menos 1280 octetos; se recomienda que sean configurados con una MTU de 1500 octetos o mayor, para alojar posibles encapsulaciones (es decir, tunelizar) sin incurrir en la fragmentación de la capa IPv6.

De cada enlace al cuál un nodo se conecta directamente, el nodo debe poder aceptar paquetes tan grandes como la MTU de ese enlace

Se recomienda fuertemente que los nodos IPv6 implementen el Descubrimiento de la MTU de la Ruta [RFC-1981] con el propósito de descubrir y tomar ventaja de las rutas con MTUs mayores que 1280 octetos. Sin embargo, una implementación IPv6 mínima (por ejemplo, en una ROM de inicio) puede restringirse simplemente a enviar paquetes no más grandes que 1280 octetos, y omitir la implementación del Descubrimiento de la MTU de la Ruta.

Con el propósito de enviar un paquete más grande que la MTU de la ruta, un nodo puede utilizar la cabecera Fragmento IPv6 para

fragmentar el paquete en el origen y tenerlo reensamblado en el(los) destino(s). Sin embargo, el uso de tal fragmentación se desalienta en cualquier aplicación que pueda ajustar sus paquetes para satisfacer la MTU de la ruta medida (es decir, por debajo de los 1280 octetos).

Un nodo debe poder aceptar un paquete fragmentado que, después del reensamblaje, sea tan grande como de 1500 octetos. Se permite a un nodo aceptar paquetes fragmentados de tal manera que reensamblan a más de 1500 octetos. Un protocolo o aplicación de capa superior que depende de la fragmentación IPv6 para enviar paquetes más grandes que la MTU de una ruta no debe enviar paquetes más grandes que 1500 octetos a menos que tenga la certidumbre que el destino es capaz reensamblar paquetes de esos tamaños tan grandes.

En contestación a un paquete IPv6 que se envía a un destino IPv4 (es decir, un paquete que experimenta la traducción del IPv6 al IPv4), el nodo IPv6 originante puede recibir un mensaje ICMP Paquete Demasiado Grande reportando de una MTU del Salto Siguiente menor a 1280. En ese caso, no se exige que el nodo IPv6 reduzca el tamaño de los paquetes subsiguientes a menos de 1280, pero debe incluir una cabecera Fragmento en esos paquetes para que el enrutador traductor de IPv6 a

IPv4 pueda obtener un valor Identificación apropiado para usar en los fragmentos IPv4resultantes. Note que esto significa que la carga útil puede tener que ser reducida a 1232 octetos (1280 menos 40 para la cabecera IPv6 y 8 para la cabecera Fragmento), y más pequeña todavía

si se usan cabeceras de extensión adicionales.

6. Etiquetas de Flujo

El campo Etiqueta de Flujo de 20 bits en la cabecera IPv6 puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por los enrutadores IPv6, tal como la calidad de servicio no estándar o el servicio en "tiempo real". Este aspecto del IPv6 está, al momento de escribir, todavía experimental y sujeto a cambio conforme los requisitos para dar soporte a flujos en la Internet se vuelvan más claros. Se exige a los hosts o a los enrutadores que no dan soporte a las funciones del campo Etiqueta de Flujo poner el campo a cero al originar un paquete,

pasar el campo inalterado al reenviar un paquete, e ignorar el campo al recibir un paquete.

El Apéndice A describe la semántica y uso del campo etiqueta de flujo pretendido en vigencia.

7. Clases de Tráfico

El campo de 8 bits Clase de Tráfico en la cabecera IPv6 está disponible para usarse por nodos originantes y/o enrutadores reenviantes para identificar y distinguir entre las diferentes clases o prioridades de paquetes IPv6. En el momento en que esta especificación está siendo escrita, hay un cierto numero de experimentos en camino en cuanto al uso de los bits Tipo de Servicio IPv4 y/o Anterioridad para proporcionar varias formas de "servicio diferenciado" para paquetes IP, además de a través del uso de un flujo establecido explícito. El campo Clase de Tráfico en la cabecera IPv6 esta proyectado para permitir similar funcionalidad que será soportada en el IPv6.

Se espera que esos experimentos conduzcan eventualmente hacia un acuerdo en que orden las clasificaciones de tráfico son mas útiles para los paquetes IP. Las definiciones detalladas de la sintaxis y semántica de todos o algunos de los bits Clase de Tráfico IPv6, si es experimental o proyectado para eventual estandarización, serán proporcionados en documentos separados.

Los siguientes requisitos generales se aplican al campo Clase de Tráfico:

o La interface de servicio para el servicio IPv6 dentro de un nodo debe proporcionar un medio para que un protocolo de capa superior proporcione el valor de los bits Clase de Tráfico en los paquetes originados por ese protocolo de capa superior. El valor por defecto debe ser cero para todos los 8 bits.

o Los nodos que soportan un uso (experimental o estándar eventual) especifico de algunos o todos los bits Clase de Tráfico se les permite cambiar el valor de esos bits en los paquetes que ellos originan, reenvían, o reciben, como sea requerido para ese uso específico. Los nodos deben ignorar y dejar sin alterar a cualesquiera de los bits del campo Clase de Tráfico para los cuales no dan soporte a un uso específico.

o Un protocolo de capa superior no debe asumir que el valor de los bits Clase de Tráfico en un paquete recibido son los mimos que el valor enviado por el origen del paquete

8. Problemas de Protocolo de Capa Superior

8.1 Sumas de Verificación de Capa Superior

Cualquier protocolo de transporte u otro de capa superior que incluya las direcciones de la cabecera IP en su cálculo de suma de

verificación debe modificarse para el uso sobre el IPv6, para incluir las direcciones IPv6 de 128 bits en lugar de las direcciones IPv4 de 32 bits. En particular, la siguiente ilustración muestra la "pseudo cabecera" TCP y UDP para el IPv6:

- Si el paquete IPv6 contiene una cabecera Enrutamiento, la Dirección Destino usada en la pseudo cabecera es la del destino final. En el nodo originante, esa dirección estará en el último elemento de la cabecera Enrutamiento; en el(los) receptor(res), esa dirección estará en el campo Dirección Destino de la cabecera IPv6.

- El valor Cabecera Siguiente en la pseudo cabecera identifica el protocolo de capa superior (por ejemplo, 6 para el TCP, o 17 para el UDP). Diferirá del valor Cabecera Siguiente en la cabecera IPv6 si hay cabeceras de extensión entre la cabecera IPv6 y la cabecera de capa superior.

- La Longitud del Paquete de Capa Superior en la pseudo cabecera es la longitud de la cabecera de capa superior y los datos (por ejemplo, la cabecera TCP más los datos TCP). Algunos protocolos de capa superior llevan su propia información de longitud (por ejemplo, el campo Longitud en la cabecera UDP); para tales protocolos, esa es la longitud usada en la pseudo cabecera.

Otros protocolos (como el TCP) no llevan su propia información de longitud, en cuyo caso la longitud usada en la pseudo cabecera es la Longitud de la Carga Útil de la cabecera IPv6, menos la longitud de cualquier cabecera de extensión presente entre la cabecera IPv6 y la cabecera de capa superior.

o A diferencia del IPv4, cuando los paquetes UDP son originados por un nodo IPv6, la suma de verificación UDP no es opcional. Es decir, siempre que se origine un paquete UDP, un nodo IPv6 debe calcular una suma de verificación UDP sobre el paquete y la pseudo cabecera, y, si ese cálculo produce un resultado de cero, debe cambiarse al hexadecimal FFFF para la colocación en la cabecera UDP. Los receptores IPv6 deben descartar los paquetes UDP que contengan una suma de verificación cero, y deben registrar el error.

La versión IPv6 del ICPM [ICMPv6] incluye la pseudo cabecera citada arriba en su cálculo de suma de verificación; éste es un cambio a diferencia de la versión IPv4 del ICMP, el cual no incluye una pseudo cabecera en su suma de verificación. La razón para el cambio es para proteger al ICMP de una mala entrega o corrupción de aquellos campos

de la cabecera IPv6 de los que depende, los qué, a diferencia del IPv4, no son cubiertos por una suma de verificación de la capa internet. El campo Cabecera Siguiente en la pseudo cabecera para el

ICMP contiene el valor 58, que identifica la versión IPv6 del ICMP.

8.2 Tiempo de Vida Máximo de un Paquete

A diferencia del IPv4, no se exigen a los nodos IPv6 cumplir con el tiempo de vida máximo de un paquete. Ésa es la razón por la que el campo "Tiempo de Vida" del IPv4 se renombró a "Límite de Saltos" en el IPv6. En la práctica, muy pocas, si alguna, implementaciones IPv4 adoptan el requisito de limitar el tiempo de vida de un paquete, asi que esto no es un cambio en la práctica. Cualquier protocolo de capa superior que depende de la capa internet (ya sea IPv4 o IPv6) para limitar el tiempo de vida de un paquete debe actualizarse para proporcionar sus propios mecanismos de detección y descarte de paquetes obsoletos.

8.3 Tamaño Máximo de la Carga Útil de Capa Superior

Al calcular el tamaño máximo de carga útil disponible para los datos de capa superior, un protocolo de capa superior debe tener en cuenta el tamaño más grande de la cabecera IPv6relativo a la cabecera IPv4. Por ejemplo, en el IPv4, la opción MSS del TCP se calcula como el tamaño máximo de paquete (un valor por defecto o un valor aprendido a través del Descubrimiento de la MTU de la Ruta) menos 40 octetos (20

octetos para la longitud mínima de la cabecera IPv4 y 20 octetos para la longitud mínima de la cabecera TCP). Al usar TCP sobre IPv6, el MSS debe calcularse como el tamaño máximo de paquete menos 60 octetos, puesto que la longitud mínima de la cabecera IPv6 (es decir, una cabecera IPv6 sin cabeceras de extensión) es 20 octetos más larga

que la longitud mínima de la cabecera IPv4.

8.4 Contestando a Paquetes que Llevan Cabeceras Enrutamiento

Cuando un protocolo de capa superior envía uno o más paquetes en contestación a un paquete recibido que incluía una cabecera Enrutamiento, el(los) paquete(s) respuesta no debe(n) incluir una cabecera Enrutamiento que se derivó automáticamente "invirtiendo" la

cabecera Enrutamiento recibida A MENOS QUE se hayan verificado la integridad y autenticidad tanto de la Dirección Origen como de la cabecera Enrutamiento recibida (por ejemplo, mediante el uso de una cabecera Autenticación en el paquete recibido). En otras palabras, se permiten sólo los siguientes tipos de paquetes en contestación a un paquete recibido que lleva una cabecera Enrutamiento:

- Los paquetes respuesta que no llevan cabeceras Enrutamiento.

- Los paquetes respuesta que llevan cabeceras Enrutamiento que NO

se derivaron invirtiendo la cabecera Enrutamiento del paquete recibido (por ejemplo, una cabecera Enrutamiento proporcionada por configuración local).

o Los paquetes respuesta que llevan cabeceras Enrutamiento que se derivaron invirtiendo la cabecera Enrutamiento del paquete recibido SI Y SÓLO SI la integridad y autenticidad de la Dirección Origen y de la cabecera Enrutamiento del paquete recibido han sido verificadas por el contestador.

Apéndice A. Uso y Semántica del Campo Etiqueta de Flujo

Un flujo es una secuencia de paquetes enviada desde un origen determinado hacia un destino (unienvío o multienvío) determinado para

el cual el origen desea un tratamiento especial por los enrutadores intermedios. Podría transmitirse la naturaleza de ese tratamiento especial hacia los enrutadores por un protocolo control, tal como el protocolo reservación de recurso, o por información dentro de los mismos paquetes del flujo, por ejemplo, en una opción de salto a salto. Los detalles de tales protocolos control u opciones están fuera del ámbito de este documento.

Pueden haber flujos activos múltiples desde un origen hacia un destino, así como también tráfico que no esta asociado con algún flujo. Un flujo se identifica singularmente por la combinación de una

dirección origen y una etiqueta de flujo no cero. Los paquetes que no pertenecen a un flujo llevan una etiqueta de flujo de cero.

Una etiqueta de flujo se asigna a un flujo en el nodo origen del flujo. Deben escogerse nuevas etiquetas de flujo (pseudo) aleatoriamente y uniformemente del rango 1 al FFFFF en hexadecimal.

El propósito de la asignación al azar es para hacer cualquier conjunto de bits dentro del campo Etiqueta de Flujo adecuado para el uso como una clave por los enrutadores, para buscar el estado asociado con el flujo.

Deben enviarse todos los paquetes que pertenecen al mismo flujo con la misma dirección origen, dirección destino, y etiqueta de flujo. Si alguno de esos paquetes incluye una cabecera Opciones de Salto a Salto, entonces todos ellos deben originarse con los mismos contenidos de cabecera Opciones de Salto a Salto (excepto el campo Cabecera Siguiente de la cabecera Opciones de Salto a Salto). Si alguno de esos paquetes incluye una cabecera Enrutamiento, entonces todos ellos deben originarse con los mismos contenidos en todas las cabeceras de extensión e incluso la cabecera Enrutamiento (excepto el campo Cabecera Siguiente en la cabecera Enrutamiento). Se permiten a los enrutadores o destinos, pero no se exige, verificar que estas

condiciones se cumplen. Si una violación se detecta, debe reportarse al origen en un mensaje ICMP Problema de Parámetro, Código 0, apuntando al octeto de mayor orden del campo Etiqueta de Flujo (es decir, desplazamiento 1 dentro del paquete IPv6).

El tiempo de vida máximo de cualquier flujo en estado de tratamiento establecido a lo largo de la ruta de un flujo debe especificarse como parte de la descripción del estado del mecanismo de establecimiento, por ejemplo, el protocolo reservación de recurso o la configuración de la opción de salto a salto de flujo. Un origen no debe reusar una etiqueta de flujo para un nuevo flujo dentro del tiempo de vida máximo de cualquier flujo en estado de tratamiento que se podría haber establecido para el uso anterior de esa etiqueta de flujo Cuando un nodo detiene y reinicia (por ejemplo, como resultado de una

"caída"), debe tener el cuidado de no usar una etiqueta de flujo que podría haber usado para un flujo anterior cuyo tiempo de vida pueda no haber expirado aún. Esto puede lograrse registrando el uso de las etiquetas de flujo sobre un almacenamiento estable para que pueda tenerse presente durante las caídas, o absteniéndose de usar cualquier etiqueta de flujo hasta que el tiempo de vida máximo de cualquier posible flujo previamente establecido haya expirado. Si se conoce el tiempo mínimo para reinicializar el nodo, ese tiempo puede descontarse del periodo de espera necesario antes de empezar a asignar las etiquetas de flujo.

No hay ningún requisito que todos, o incluso la mayoría, de los paquetes pertenezcan a flujos, es decir, que lleven etiquetas de flujo no cero. Esta observación se pone aquí para recordar a los diseñadores e implementadores de protocolos no asumir lo contrario. Por ejemplo, sería desacertado diseñar un enrutador cuyo rendimiento sólo sería adecuado si la mayoría de los paquetes pertenecieran a flujos, o diseñar un esquema de compresión de cabecera que sólo trabaje sobre paquetes que pertenezcan a flujos.

Apéndice B. Pautas de Formateo para las Opciones

Este apéndice da algunos consejos en cómo disponer los campos al diseñar nuevas opciones para ser usadas en la cabecera Opciones de Salto a Salto o en la cabecera Opciones de Destino, tal como se describe en la sección 4.2. Estas pautas se basan en las siguientes suposiciones:

- Una característica deseable es que cualquier campo multiocteto dentro del área Datos de la Opción de una opción se alinean en

sus límites naturales, es decir, los campos de ancho de n octetos deben ser colocados en un entero múltiplo de n octetos desde el inicio de la cabecera Opciones de Salto a Salto o de la cabecera Opciones de Destino, para n = 1, 2, 4, o 8.

o Otra característica deseable es que la cabecera Opciones de Salto a Salto o la cabecera Opciones de Destino ocupe tan poco espacio como sea posible, sujeto al requisito que la cabecera sea un entero múltiplo de 8 octetos de largo.

o Puede asumirse que, cuando ambas cabeceras que tienen opciones están presentes, llevan un número muy pequeño de opciones, usualmente solo una.

Estas suposiciones sugieren la siguiente propuesta para disponer los campos de una opción: ordenar los campos desde el más pequeño hasta el más grande, sin relleno interior, luego deducir el requisito de alineación para la opción entera en base al requisito de alineación del campo más grande (hasta una alineación máxima de 8 octetos). Esta propuesta se ilustra en los siguiente ejemplos:

Ejemplo 1

Si una opción X requiere dos campos datos, uno de longitud de 8

octetos y uno de longitud de 4 octetos, se dispondrían tal como sigue:

Su requisito de alineación es 8n+2, para asegurar que el campo de 8 octetos comience en un desplazamiento múltiplo de 8 a partir del inicio de la cabecera circundante. Una cabecera Opciones de Salto a Salto completa o una cabecera Opciones de Destino completa que contiene esta única opción se vería como sigue:

Ejemplo 2

Si una opción Y requiere tres campos datos, una de longitud de 4 octetos, una de longitud de 2 octetos, y una de longitud de 1 octeto, se dispondrían tal como sigue:

Su requisito de alineación es 4n+3, para asegurar que el campo de 4 octetos comience en un desplazamiento múltiplo de 4 a partir del inicio de la cabecera circundante. Una cabecera Opciones de Salto a Salto completa o una cabecera Opciones de Destino completa que contiene esta única opción se vería como sigue

Ejemplo 3

Una cabecera Opciones de Salto a Salto o una cabecera Opciones de Destino que contiene ambas opciones X e Y de los Ejemplos 1 y 2 tendría uno de los dos siguientes formatos, dependiendo en que opción apareciera primero:

Consideraciones de Seguridad

Las características de seguridad del IPv6 se describen en la Arquitectura de Seguridad para el Protocolo Internet [RFC-2401].

Reconocimientos

Los autores agradecidamente reconocen el gran número de sugerencias útiles de los miembros del grupo de trabajo IPng, del grupo de investigación de Protocolos de Extremo a Extremo, y de la Comunidad Internet En General.

Direcciones de los Autores

Stephen E. Deering

Cisco Systems, Inc.

170 West Tasman Drive

San Jose, CA 95134-1706

USA

Teléfono: +1 408 527 8213

Fax: +1 408 527 8254

Correo Electrónico: deering@cisco.com

Robert M. Hinden

Nokia

232 Java Drive

Sunnyvale, CA 94089

USA

Teléfono: +1 408 990-2004

Fax: +1 408 743-5677

Correo Electrónico: hinden@iprg.nokia.com

Dirección del Traductor al Castellano

Percy Luis Ché Castillo

UPAO

Av. América Sur 3145

Urb. Monserrate, Trujillo

PERÚ

Teléfono: +51 044 201880

Fax: +51 044 286111

Correo Electrónico: percychecastillo@yahoo.com

Referencias

[RFC-2401] Kent, S. y R. Atkinson, "Arquitectura de Seguridad para el Protocolo Internet", RFC 2401, Noviembre 1998.

[RFC-2402] Kent, S. y R. Atkinson, "Cabecera Autenticación del IP", RFC 2402, Noviembre 1998.

[RFC-2406] Kent, S. y R. Atkinson, "Seguridad del Encapsulado de la Carga Útil (ESP)", RFC 2406, Noviembre 1998.

[ICMPv6] Conta, A. y S. Deering, "ICMP para el Protocolo Internet Versión 6 (IPv6)", RFC 2463, Diciembre 1998.

[ADDRARCH] Hinden, R. y S. Deering, "Arquitectura de Direccionamiento para la Versión 6 del IP", RFC 2373, Julio 1998.

[RFC-1981] McCann, J., Mogul, J. y S. Deering, "Descubrimiento de la MTU para la versión 6 del IP", RFC 1981, Agosto 1996.

[RFC-791] Postel, J., "Protocolo Internet", STD 5, RFC 791, Setiembre 1981.

[RFC-1700] Reynolds, J. y J. Postel, "Números Asignados", STD 2, RFC 1700, Octubre 1994. Ver también: http://www.iana.org/numbers.html

[RFC-1661] Simpson, W., "El Protocolo Punto a Punto (PPP)", STD

51, RFC 1661, Julio 1994.

CAMBIOS A PARTIR DE LA RFC-1883

Este memorándum tiene los siguientes cambios a partir de la RFC-1883.

Los números identifican la versión del Bosquejo Internet en la cual se hizo el cambio.

02) Se quitaron todas las referencias a datagramas de tamaño gigante y la opción Carga Útil de Tamaño Gigante (se movió hacia un documento separado).

02) Se movió la mayor parte de la descripción de la Etiqueta de Flujo de la sección 6 hacia el (nuevo) Apéndice A.

02) En la descripción de la Etiqueta de Flujo, ahora en el Apéndice A, se corrigió el valor Etiqueta de Flujo máximo de FFFFFF a FFFFF (es decir, un "F" menos) debido a la reducción del tamaño del campo Etiqueta de Flujo de 24 bits a 20 bits.

02) Se reenumeró (se reletreó?) el anterior Apéndice A para ser el

02) Se cambió la redacción de la sección Consideraciones de Seguridad para evitar bucle dependencia entre esta especificación y las especificaciones del IPsec.

02) Se actualizó la dirección de correo electrónico y la afiliación de compañía de R. Hinden.

01) En la sección 3, se cambió el nombre del campo "Clase" a "Clase de Tráfico" y se aumentó su tamaño de 4 a 8 bits. Se disminuyó el tamaño del campo Etiqueta de Flujo de 24 a 20 bits para compensar el aumento en el campo Clase de Tráfico.

01) En la sección 4.1, se restituyó el orden de la Cabecera Autenticación y la Cabecera ESP, las cuales fueron intercambiadas equivocadamente en la versión 00 de este memorándum.

01) En la sección 4.4, se suprimió el campo Mapa de Bits Estricto/Impreciso y la funcionalidad enrutamiento estricto de la cabecera Enrutamiento de Tipo 0, y se quitó la restricción sobre el número de direcciones que pueden ser llevadas dentro de

la cabecera Enrutamiento de Tipo 0 (fue limitado a 23 direcciones, debido al tamaño del mapa de bits estricto/impreciso).

01) En la sección 5, se cambió la mínima MTU IPv6 de 576 a 1280 octetos, y se añadió una recomendación que los enlaces con una MTU configurable (por ejemplo, enlaces PPP) sean configurados para tener una MTU de por lo menos 1500 octetos.

01) En la sección 5, se suprimió el requisito que un nodo no debe enviar paquetes fragmentados de tal manera que reensamblan a más de 1500 octetos sin conocimiento del tamaño del búfer de reensamblaje destino, y se lo reemplazó con una recomendación que los protocolos o las aplicaciones de capa superior no deberían hacer eso.

01) Se reemplazó la referencia hacia la especificación Descubrimiento de la MTU de la Ruta para el IPv4 (RFC-1191) con la referencia hacia la especificación Descubrimiento de la MTU de la Ruta para el IPv6 (RFC-1981), y se suprimieron las Notas al final de la sección 5 respecto al Descubrimiento de la MTU de la Ruta, dado que esos detalles ahora son cubiertos por la RFC-1981.

01) En la sección 6, se suprimió la especificación de flujo establecido "oportunista", y se quitaron todas las referencias al tiempo de vida máximo de 6 segundos para el estado de flujo establecido oportunamente.

01) En la sección 7, se suprimió la descripción provisional de la estructura interna y semántica del campo Clase de Tráfico, y se especificó que tales descripciones sean proporcionadas en documentos separados.

00) En la sección 4, se corrigió el valor Código para indicar "encontrado tipo de Cabecera Siguiente desconocido" en un mensaje ICMP Problema de Parámetro (se cambió de 2 a 1).

00) En la descripción del campo Longitud de la Carga Útil en la sección 3, y del campo Longitud de la Carga Útil de Tamaño Gigante en la sección 4.3, se aclaró que las cabeceras de extensión están incluidas en el conteo de la longitud de la carga útil.

00) En la sección 4.1, se intercambió el orden de la cabecera

Autenticación y la cabecera ESP. (NOTA: esto fue un error, y el cambio fue desecho en la versión 01).

00) En la sección 4.2, se aclaró que las opciones son identificadas por un Tipo de Opción de 8 bits completo, no por los 5 bits de bajo orden de un Tipo de Opción. Se especificó también que el mismo espacio de enumeración del Tipo de Opción es usado tanto por la cabecera Opciones de Salto a Salto como por la cabecera Opciones de Destino.

00) En la sección 4.4, se añadió una sentencia exigiendo que los nodos que procesan una cabecera Enrutamiento deben enviar un mensaje ICMP Paquete Demasiado Grande en contestación a un paquete que es demasiado grande para caber en el enlace de salto siguiente (en lugar de, digamos, llevar a cabo fragmentación).

00) Se cambió el nombre del campo Prioridad IPv6 a "Clase", y se reemplazó la descripción anterior de Prioridad en la sección 7 con una descripción del campo Clase. También, se excluyó este campo del conjunto de campos que deben permanecer de la misma forma para todos los paquetes en el mismo flujo, tal como se especificó en la sección 6.

00) En la pseudo cabecera en la sección 8.1, se cambió el nombre del campo "Longitud de la Carga Útil" a "Longitud del Paquete de Capa Superior". Se aclaró también que, en el caso de protocolos que llevan su propia información de longitud (como el datagrama de tamaño no gigante UDP), es la longitud derivada de la capa superior, no la longitud derivada de la capa IP, la que es usada en la pseudo cabecera.

00) Se añadió la sección 8.4, especificando que los protocolos de capa superior, al contestar a un paquete recibido que llevó una cabecera Enrutamiento, no deben incluir el inverso de la cabecera Enrutamiento en el(los) paquete(s) respuesta a menos que la cabecera Enrutamiento recibida fuese autenticada.

00) Corregidos algunos errores tipográficos y errores gramaticales.

Declaración de Copyright Completa

Borradores de IPv6:

La tabla siguiente muestra los Borradores del protocolo IPv6, según han sido presentados al IETF:

	Borrador IETF	Título
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 clientes IPv4
	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
Multi-Homing	ipngwg-default-addr-select-00.txt	Selección de Direcciones por Defecto para IPv6
	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 basados en SOCKS
	ngtrans-6bone-6papa-01.txt	Pre-cualificación para asignación de prefijos de direcciones en 6Bone (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
	pim-v2-sm-01.txt	Protocolo de Routing Multicast Independiente en Modo Esparcido (PIM-SM)

Situación Mundial de Ipv6

1. Introducción

Desde Julio del 99, podemos afirmar que IPv6 no es una teoría, sino un hecho.

La razón ha sido la constitución, por parte de los más importantes jugadores de la industria, de una asociación sin ánimo de lucro, "*el Foro IPv6*", con el objetivo común de educar al mercado en las ventajas del protocolo IPv6, promover su uso, y reforzar su aplicación en el mundo.

La lista de corporaciones involucradas en este proyecto es una mezcla explosiva, incluyendo fabricantes, instituciones de Investigación y Desarrollo, organizaciones de Educación, Operadores de Telecomunicaciones, y Empresas de Consultoría, entre otros.

Eso implica, por supuesto, una ingente generación de esfuerzos personales y de corporaciones, presionando a las Organizaciones de Normalización para acelerar el proceso, para culminar con la creación de una definición completa y estable del protocolo.

Permítanme introducirles en el Foro IPv6 y la situación actual del protocolo a través del mundo.

2. La Constitución del Foro IPv6: Nota de Prensa

El contenido oficial de la Nota de Prensa fue:

Ha sido creado el Nuevo Foro de Internet: El FORO IPv6

Luxemburgo, 7 de Julio de 1999. Un consorcio mundial de líderes proveedores de soluciones Internet, Proveedores de Servicios Internet (PSI's) y redes de investigación y educación, se han unido para formar el FORO IPv6. Este FORO tiene la clara misión de promover IPv6 (Protocolo Internet versión 6) para crear la próxima generación de Internet, de mayor calidad y más segura: La NUEVA INTERNET. El FORO planea mejorar dramáticamente la promoción de IPv6 hacia el mercado y los usuarios proporcionando acceso libre, global y equitativo a los conocimientos y la tecnología. El FORO trabajará estrechamente ligado a IETF (Internet Engineering Task Force) responsable de las especificaciones técnicas de IPv6 y al cual muchos miembros del FORO contribuyen.

"IPv6 esta aquí y ahora, illevemos por tanto Internet a donde ninguna otra red ha llegado nunca!", comenta el Dr. Vint Cerf, Presidente de la IETF y reconocido como unos de los padres de Internet.

"Durante algunos años hemos reconocido que la versión 4 de IP está alcanzando sus límites, y la IETF ha estado trabajando en IPv6 desde 1994. Ahora, las especificaciones básicas han sido acordadas e implementadas, y es el momento de seguir adelante" añade el Dr. Brian E. Carpenter, Presidente del comité de Arquitectura de Internet de la, y Director de Programa en la División Internet de IBM.

"Hemos sido muy activos en la construcción de una fuerte infraestructura IPv6 en Japón porque prevemos importantes beneficios inmediatos para nuestra economía, conocimientos y potencial educativo para nuestra gente" confirma el Dr. Jun Murai, Director General del proyecto WIDE IPv6 y Profesor de la Universidad de KEIO.

"Nokia considera que IPv6 es un activador fundamental para la visión que tenemos de la Sociedad de Información Móvil. Actualmente, el número de teléfonos móviles ya supera con creces el número de terminales fijos de Internet; IPv6 es la única arquitectura viable que puede acomodar la nueva ola de dispositivos celulares capaces de Internet. Nokia está ansiosa de contribuir a los esfuerzos del Foro IPv6 para acelerar la aceptación y el empleo de IPv6 a través de Internet" indica Pekka Ala-Pietilä, Presidente de Nokia.

"Ericsson tiene una clara visión de negocio y tecnología acerca de cómo IPv6 permite la oferta de servicios y prestaciones demandados por las infraestructuras móviles (GPRS, UMTS), redes de banda ancha, electrónica de consumo y terminales, y la subsecuente interoperatibilidad/gestión, extendiendo por tanto, nuestro completo soporte al Foro IPv6 ", enfatiza Jan Uddenfeldt, Vicepresidente Senior y Director Técnico de L.M.Ericsson.

"Los nobles objetivos del Foro IPv6 serán la promoción mundial de esta nueva tecnología, compartiendo conocimientos, experiencias e interoperatibilidad y creando bases comunes para la Nueva Internet del próximo milenio", afirma Latif Ladid, Presidente del FORO IPv6 y Vicepresidente de Telebit Communications.

Miembros Fundadores del Foro IPv6

Entre los miembros iniciales del Foro IPv6 se incluyen 42 de las compañías e instituciones punteras activas en la nueva tecnología Internet, un foro verdaderamente internacional desde el primer día:

Europa y Medio Este (18): BT, Case Technology, Consulintel, Deutsche Telekom, CSELT, DFN, Ericsson, Eurocontrol, Gigabell, IABG, Intracom, Netmedia, Nokia, Teldat, Telebit Communications, CSELT, Telia Networks Services, Thomson-CSF Detexis.

Norte América (18): 3Com, Advanced Systems Consulting, AT&T, Cisco, Compaq, ESNet, Hewlett-Packard, IBM, MCI WorldCom, Mentat, Microsoft, Motorola, Qwest, SGI, Sprint, Sun, The Business Internet, Viagenie-Canarie.

Asia (6): Centre for Wireless Communications (Singapore), Hitachi, NTT, NTT Software Corporation, Trumpet Software, WIDE Japan.

Para más detalles acerca de la Tecnología IPv6 o para inscribirse en el Foro IPv6, visite, por favor, la Página Web del FORO IPv6:

http://www.ipv6forum.com

En esta nota de prensa, descubrimos el alto nivel de apoyo, desde el inicio, para este objetivo, por parte de compañías locales, internacionales y multinacionales, así como por destacados profesionales y relevantes personalidades en

Internet (incluyendo al Dr. Vinton Cerf, Presidente Honorario), en todo el mundo.

Sólo como "medida" de la importancia del protocolo IPv6 para el mercado, podemos mencionar una anécdota acerca del número de miembros en la constitución del Foro. Se han alcanzado los 42 miembros fundadores en unas pocas semanas, mientras que unos años atrás, conseguir el mismo número de miembros para el Foro RDSI, llevó más de 2 años. No hace falta mencionar, como comparativa, la importancia que la tecnología RDSI ha jugado en los últimos años en el mercado mundial de las telecomunicaciones.

3. **Los miembros del Foro IPv6**

El estado actual de los miembros del Foro IPv6, fechado a 10 de Enero del 2000, es de 73 compañías/organizaciones:

1 - Case Technology, UAE
2 - Thomson-CSF Detexis, France
3 - Ericsson Telebit, Denmark
4 - Eurocontrol, France
5 - Gigabell, Germany
6 - Hitachi, Japan
7 - Hewlett-Packard, US
8 - DFN, Germany
9 - Canarie-Viagenie, Canada
10- NTT, Japan
11- WIDE, Japan
12- BT, UK
13- CSELT, Italy
14- Mentat, US
15- SUN, US
16- Netmedia, Finland
17- Trumpet Software, Australia
18- Intracom, Greece
19- Cisco, US
20- COMPAQ, US
21- SPRINT, US
22- NOKIA, US
23- AT&T, US
24- Teldat, Spain
25- Deutsche Telekom, Germany
26- Qwest, US
27- IABG, Germany
28- ESnet-6REN, US
29- MCI WorldCom, US
30- Ericsson, Sweden

31- Microsoft, US
32- 3Com, US
33- Advanced Systems Consulting, Inc., US
34- Consulintel, Spain
35- The Business Internet, US
36- NTT Software Corporation, Japan
37- Motorola, US
38- Telia Networks Services, Sweden
39- Centre for Wireless Communications, Singapore
40- Siemens, Germany
41- IBM, US
42- BellSouth, US
43- Teleglobe, US
44- Silicon Graphics, Inc (SGI), US
45- Etisalat, UAE
46- SwitchCore AB, Sweden
47- UCAID - Internet2, US
48- University College of London (UCL), UK
49- University of Southampton, United Kingdom
50- University of Lancaster, United Kingdom
51- Royal Philips - The Netherlands
52- Royal KPN (Royal Dutch Telecom) - The Netherlands
53- The Open Group - UK
54- CIAC, France
55- UNINETT, Norway
56- NEC, Japan
57- ETRI, Korea
58- INTAP, Japan
59- Alpha Group, US
60- Korea Telecom, Korea
61- CNRS, France
62 -YDC (Yokogawa Digital Computer Corporation), Japan
63 - Alcatel, France
64 - GITEP, France
65 - ISI, US - UK
66 - Nortel Networks - US
67 - ISOC
68 - Stardust.com, US
69 - Telefonica Spain
70 - Telscom, CH
71 - NFP, Finland
72 - Lucent, EU/US
73 - IMAG, France

Otras compañías en proceso de incorporación, a la espera de procedimiento internos de aprobación son:

1 - France Telecom - France
2 - Apple - US
3 - SPAWAR - US

El listado, recopilado en el orden en que estas corporaciones se han ido uniendo al Foro, se mantiene actualizado en la Web del propio Foro:
http://www.ipv6forum.com/navbar/members/foundingmembers.htm (miembros fundadores) y
http://www.ipv6forum.com/navbar/members/generalmembers.htm (miembros generales).

4. Objetivos del Foro IPv6:

Según las palabras de Latif Ladid, Presidente del Foro IPv6, lo definimos como un consorcio mundial de proveedores líderes de Internet, Redes de Educación e Investigación, con la clara misión de promocionar IPv6 mejorando dramáticamente el reconocimiento de IPv6 por parte del mercado y los usuarios, creando la Nueva Generación de Internet con calidad y seguridad y permitiendo 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 desarrollara el protocolo, dado que la única autoridad competente para esta misión es el IETF (Internet Engineering Task Force).

1. Estructura del Foro IPv6

El Foro IPv6 ha sido organizado en dos "cuerpos" principales, ambos dependiendo del *Consejo del Foro IPv6*:

- *Directiva Técnico de Despliegue de IPv6.*

Este directiva tiene plena autonomía en sus decisiones respecto del grupo de promoción, garantizando soluciones técnicas objetivas e independientes de fabricantes. Esta disponible para la asistencia a los miembros del Foro en cuestiones y oportunidades técnicas, de despliegue e implementación.
La directiva consiste en unos 20 miembros "contribuidores activos", con el fin de cubrir una amplia experiencia en áreas como seguridad, routing, movilidad, QoS, entornos de PC, software de fuentes abiertas, gestores de redes, desarrolladores de aplicaciones, verificación y prueba, telefonía IP, etc.

- *Grupo de Promoción del Foro IPV6.*

El Grupo de Promoción se compone de los siguientes *Grupos de Trabajo* (siempre abiertos a nuevos grupos):

- Proyectos: Casos de Negocios de la Vida Real, Historias Exitosas de IPv6, Proyectos Nacionales e Internacionales, Proyectos Subvencionados, ... El objetivo es demostrar la evolución positiva hacia la Nueva Internet con proyectos colaborativos trabajando sobre tecnología IPv6, facilitando el intercambio de información entre proyectos y la creación de otros nuevos.
- Educación, Promoción y Relaciones Públicas. El objetivo es crear y promover, por cualquier medio, mensajes de calidad, documentos, presentaciones, y herramientas, para educar-evangelizar acerca de IPv6 y asegurarse destacar una imagen limpia y poderosa de las ventajas de IPv6.
- Conferencias Globales de IPv6: Encuentros/Conferencias Internacionales y Regionales de IPv6, Conferencias de Asociados, ... El objetivo es crear eventos mundiales y locales para promocionar diversos aspectos de IPv6.
- Programa de Embajadores: Forma alternativa, sin coste, para individuos que desean participar en la promoción del protocolo IPv6. Destinado a gente interesada en escribir artículos, realizar presentaciones, discursos, u otras actividades promocionales/educacionales, fundamentalmente locales.

1. Eventos y Conferencias del Foro IPv6

El primer encuentro "oficial" del Foro IPv6 fue en Oslo, en Julio de 1999, junto al encuentro del IETF. Este fue más un encuentro de "constitución" que un evento público.

Tras este, la 1ª Conferencia IPv6 tuvo lugar en París, durante Octubre de 1999. Fue un gran evento muy exitoso.

En Diciembre de 1999, tuvo lugar el siguiente encuentro en Berlín.

Los eventos planeados para el año 2000 incluyen Telluride (Colorado, US, Marzo), Birmingham (UK, Mayo), Tokio (Japón, Julio).

Por supuesto, el evento que más nos compete es el que celebraremos en Madrid, el 29-30 de Noviembre y 1 de Diciembre del 2000, con importantes ponentes locales e internacionales. Para recibir más información acerca del mismo, preinscríbanse sin compromiso en http://www.consulintel.es/Html/ForoIPv6/foroipv6.htm.

El Foro IPv6 esta abierto a cualquier cooperación para preparar este tipo de eventos, independientemente de que sean locales o internacionales.

2. Cooperación del Foro IPv6 con otras instituciones

Como complemento a sus objetivos promocionales, el Foro IPv6 mantiene las puertas abiertas a acuerdos con otras instituciones o Foros Industriales.

De hecho, ya se han establecido acuerdos de colaboración muy estrechos con el Foro UMTS, el Foro GSM, ISOC, y ETSI, entre otros.

Como resultado directo de esta colaboración, el Foro IPv6 participa y participará en otros eventos: UMTS Forum Workshop (Singapore, Noviembre de 1999), Next Generation Billing Systems (Cannes, Diciembre de 1999), ComNet 2000 (Washington, Enero del 2000), Mobile.ISP (París, Marzo del 2000).

3. Situación de la Definición del Protocolo IPv6

Según los expertos, en general, el protocolo IPv6 esta bien definido y el núcleo de las especificaciones es muy sólido.
Pero aún existen algunos puntos clave que necesitan trabajos adicionales:

- Problema de Multi-homing. Básicamente el mismo que tenemos en IPv4, y ¡seguimos sobreviviendo! Existen diversas propuestas al respecto, incluyendo el uso de mecanismos de movilidad IP, mecanismos de host, mecanismos de routers, ... En cualquier caso, cualquiera de estas propuestas supone retrasos en el desarrollo e implantación de IPv6.
- Todavía hay quien cuestiona que el direccionamiento de longitud fija sea la alternativa más adecuada. Pero hay que reconocer que el direccionamiento fijo de 128 bits es un límite muy difícil de superar. Actualmente, se está trabajando dentro de este límite con los formatos IPv6 agregables. Ya ha sido mundialmente aceptado, por lo que no hay necesidad de cuestionar de nuevo su redefinición.
- El Grupo de Trabajo DHC del IETF desea verificar que los modelos que están siendo usados como DHCPv6 (la arquitectura es diferente y debe incorporar la RFC 2462 - Stateless Address Configuration) son válidos y trabajarán basándose en los conocimientos adquiridos por las implementaciones DHCPv4. El Grupo de Trabajo IPng quiere extender lo que no se ha podido hacer con DHCPv4 pero sin perder los conocimientos adquiridos en este protocolo. Estos trabajos están siendo finalizados en este momento, y debe de haber un borrador muy sólido en torno a Mayo del 2000, listo para su implementación y para elevarlo a una Propuesta de Norma.
- El uso de ámbitos para unicast de direcciones IPv6, mientras se fijan los procedimientos para su uso y aplicación. Los ámbitos son perfectamente conocidos en IPv6 para unicast de direcciones globales, direcciones de enlace local, y multicast. Se está discutiendo su uso para direcciones locales y como se usarán dentro de la arquitectura, y ello afecta a las implementaciones.
- Aún es precios implementar y comprobar protocolos de Multicast bajo IPv6, dado que, desafortunadamente, aún no han sido lo suficientemente verificados. Existen trabajos en marcha para PIMv6 (Protocol Independent Multicast IPv6), pero no necesitamos esperar al routing multicast para comenzar la implantación de IPv6. Sería bueno si pudiéramos ver más implementaciones de OSPFv6, dado que tampoco ha sido lo suficientemente verificado en este momento.
- Otra reciente petición ha sido los trabajos para IS-IS para IPv6. IS-IS es un protocolo OSI que puede adaptarse a cualquier otro

protocolo mediante su encapsulado. Como IPv4, IPv6, IPX, DecNet, ...

1. Problemas de Normalización de IPv6

La mayor parte de los trabajos han sido definidos como "finalizados" tras el 45° encuentro del IETF en Oslo.

El IESG ha indicado que sólo se requiere algo más de experiencia "en campo", es decir, en aplicaciones reales.

2. ¿Es IPv6 suficiente para Calidad de Servicio extremo a extremo?

Si somos capaces de aprovechar al máximo los campos de "Clase de Tráfico" y "Flujo" ("Traffic Class" y "Flow"), es un buen comienzo, y la cabecera IPv6 proporciona una estructura inherente dentro de la propia cabecera IP.

Pero, al igual que en IPv4, la cuestión es como usan las aplicaciones la Calidad de Servicio (QoS), cuando esta se habilita aplicación por aplicación.

¿Qué significa esto? Sencillo: IPv6, por si solo, no es suficiente para cumplir este objetivo.

Siendo tan solo un protocolo de la capa de red, IPv6 sólo será capaz de proporcionar QoS de red a red, cuando se combine con los mecanismos apropiados en los routers de la red bajo una determinada aproximación para dicha calidad de servicio: Servicios "Integrated" o "Differential".

Tal y como hemos comentado, afortunadamente, IPv6 se combina bien con ambas tecnologías, y ofrece algunas mejoras respecto de IPv4, como la disponibilidad de la etiqueta de Flujo, junto a la etiqueta de Clase de Tráfico, para llevar identificaciones de "micro-flujos" para "Int-serv" o "Diff-serv".

Hay propuestas para usar estos campos o etiquetas para MPSL, en el caso de que se emplee MPSL como tecnología de "activación" de Calidad de Servicio.

Como resumen, podemos afirmar que, respecto a IPv4, la ventaja de IPv6 es que no tiene problemas "heredados", y la tremenda mayor facilidad para la clasificación de paquetes con Identificadores de tráfico.

3. Competidores de IPv6

Hay quien opina que algunas formas de direccionamiento ajustable pueden ser implementadas perfectamente, sin necesidad de mayores modificaciones. Todas las direcciones serían relativas al ámbito de la longitud en la que son usadas. En su origen, es un tipo de CLNS.

Es cierto que podría ser una buena solución, sin embargo, el procesado de las opciones de la cabecera sigue siendo una ventaja insuperable de IPv6 sobre cualquier otra solución.

El hecho es que no hay ninguna propuesta real para otros protocolos (fueron rechazadas durante el proceso de selección de IPng). Por tanto, el competidor real puede ser NAT y su descendiente, RSIP.

NAT es casi "transparente" por el hecho de intercambiar espacio de direcciones a costa de la complejidad para su gestión (este punto terminará "matando" este protocolo a largo plazo).

NAT aísla intranets de internet trabajando en contra de la carencia de direcciones. Los esquemas son revisables, dando lugar a múltiples "convertidores" NAT para proporcionar conectividad global. Sin embargo, esta aproximación esta violando el concepto general de Internet: transparencia en el ámbito de la red.

NAT incrementa la complejidad de la configuración y crea puntos únicos de fallo (cuellos de botella) en las conexiones a redes.

NAT rompe el modelo de conexión extremo a extremo (y por tanto rompe el esquema de seguridad extremo a extremo) y predispone a situaciones erróneas (por ejemplo, en la red, lo cual es nefasto para la escalabilidad).

RSIP no es transparente, necesita una actualización para cada aplicación en los nodos extremos (como IPv6) y sólo extiende la longitud real de las direcciones unos pocos bits (lo cual quiere decir que no será suficiente). Por tanto, la única ventaja real de RSIP es ¡su relación con NAT!

NAT es una ayuda para resolver los problemas de IPv4, pero ha sido comparado con islas fantásticas si pensamos que puede resolver los problemas del núcleo de IPv4 que IPv6 fija definitivamente. NAT es el principal "vendaje" y no vamos a luchar contra él, sino a coexistir hasta que IPv6 lo haga innecesario.

4. **Usuarios actuales y futuros de IPv6.**

Obviamente, los mejores objetivos para la aplicación de IPv6 son lugares donde hoy no es posible obtener direcciones IPv4, por añadido, países en desarrollo y crecimiento (dado que los mayores PSI's norteamericanos aún mantienen reservas sobre el resto del espacio de direcciones IPv4).

No hay ninguna aplicación "única" para IPv6, sólo resuelve el problema de espacio de direcciones, pero este problema no tiene ninguna otra solución real, y puede evitar que cualquier nueva aplicación con grandes necesidades de espacio de direcciones, como la telefonía IP móvil. Pero, ¿Alguien tiene dudas acerca de este hecho mismo como una aplicación "única y definitiva"? Es una realidad, que el número de teléfonos móviles ya ha crecido por encima del número de conexiones a Internet.

Cualquier aplicación que actualmente corre sobre IPv4, lo hará MEJOR sobre IPv6, con muchos recursos adicionales, y ofreciendo mejores métodos para Calidad y Clase de Servicio. ¿Qué podemos decir acerca de VoIP?

Mi propia experiencia en VoFR y VoIP en instalaciones realmente grandes es más que concluyente ... Estoy convencido acerca del éxito de IP sobre FR en el futuro, pero al mismo tiempo, estoy convencido acerca de la necesidad de utilizar VoFR mientras no seamos capaces de ofrecer una red global de "VoIPv6", quiero decir, sobre redes IP públicas, sobre Internet.

¿Usuarios? El Foro IPv6 los esta definiendo. ¡El usuario final irá primero!, dado que IPv6 crecerá desde las Intranets hacia Internet. Según aumente el número de Intranets que lo usen y empleen túneles entre ellas, y se incremente el número de fabricantes que comercialicen productos con IPv6, y el Foro IPv6 vaya haciendo su trabajo, los PSI's y los operadores irán sintiéndose más cómodos, y al mismo tiempo más obligados a migrar a IPv6.

Pero nadie migrará si no se dispone de productos. Es como el eterno problema del huevo y la gallina. Y esta es una misión fundamental del Foro IPv6.

Por suerte, en el último Evento, en Berlín, todos los grandes fabricantes se han comprometido a tener producto comercial disponible después del próximo verano. Actualmente, sólo Telebit dispone de producto comercial.

5. **Lugares de Prueba y Historias Exitosas de IPv6**

No podríamos creerlo: ¡Ya hay cientos de redes funcionando con IPv6! Con usuarios reales, corporaciones reales, instituciones de educación y desarrollo, y muchos más preparados para la puesta en marcha.

Simplemente dirigiéndonos al Web de 6Bone... podremos descubrir muchos enlaces, a lo largo de todo el planeta.

Si esto no es suficiente, como botón de muestra: 6Ren, 6Init, 6Tap, FREEnet, WIDE, US Navy, Eurocontrol.

Probablemente ninguna otra tecnología ha cosechado tantos éxitos en tan poco tiempo como IPv6.

Simplemente busque en la WWW ...

Si alguien no lo tiene lo suficientemente claro, basta con leer la prensa especializada desde el momento de la constitución del Foro IPv6. Es uno de nuestros grandes objetivos, promocionaremos estas iniciativas, iniciaremos nuevos proyectos, nuevas colaboraciones; necesitamos e involucraremos tanta gente como sea posible.

El Dr. Vinton Cerf nos acaba de confirmar que MCI WorldCom utiliza, en la red vBNS, "IPv6 nativo".

NTT ha confirmado que además de haber iniciado servicios públicos IPv6 en Japón, está creando una red mundial basada en IPv6, y ofrecerá, durante un año, servicios gratuitos en la misma, a todos los clientes interesados.

Son ejemplos más que evidentes.

6. **Situación del Despliegue de IPv6**

Hemos definido IPv6 como "La Internet del Próximo Milenio", y acabamos de estrenarlo.

El año 2000 es muchas cosas, y es el año para que los fabricantes comiencen a enviar sus prototipos. Como hemos dicho, se han comprometido a ello, e incluso algunos ya tiene productos reales, funcionando perfectamente, no son "betas".

Pero, por supuesto, gran parte de la gente que usa IPv6 lo hace a través de sistemas de túneles.

En la actualidad, en el momento de escribir estas líneas, 23 corporaciones/instituciones han recibido adjudicaciones de "subTLA". Y es solo el comienzo: ¡un muy buen comienzo!

Algunos ya han anunciado ofertas de servicios regulares, nativos, IPv6. Han tomado la iniciativa de apostar por el futuro: ¡sin duda son ganadores!

Algunos otros grandes PSI's esperarán a que los clientes quieran pagar por servicios IPv6 antes de invertir. Es su propia alternativa de negocio.

En este web puede localizar una lista permanentemente actualizada de adjudicaciones de rangos "subTLA" en producción: http://www.dfn.de/service/ipv6/ipv6aggis.html

7. Barreras para IPv6

No hay muchas, y se van resolviendo día a día:

- El problema del multi-homing.
- Los "fans" del direccionamiento ajustable en longitud.
- El propio IPv4, de alguna forma, con los "parches" como NAT.
- La falta de soporte real por parte de fabricantes de routers y software "dominantes".
- La complejidad de la migración/transición.
- Los usuarios necesitan razones comerciales "FORZADAS" para moverse a IPv6.

1. Estado actual de IPv6 a lo largo del mundo

Podemos 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 región (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 éste 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). El objetivo es 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.

Según el Dr. Vinton G. Cerf, hay una gran especulación acerca de que esto se convertirá en una gran fuerza según aumente el número de dispositivos de usuario final, como teléfonos móviles y adaptadores de televisión por cable, que requieren direccionamiento IP, lo que obligará a los desarrolladores a escoger IPv6 frente a IPv4 para permitir direcciones únicas para cada dispositivo. Este paso también supondrá, en muchos casos, el uso de NAT's (Network Address Translators), para permitir el transporte de paquetes IPv6 sobre troncales IPv4.

1. ¿Cuándo y Donde IPv6?

Tal y como hemos dicho al principio de este documento, IPv6 es un hecho.

Las primeras implementaciones estaban disponibles en 1995 (la primera señal de una conexión IPv6 está fechada al final de Marzo de 1995).

Muchos de los fabricantes de software y Sistemas Operativos tienen "pilas" IPv6 en sus productos, y otros como "kits de acceso temprano", libres de cargo, pero sin ningún soporte "oficial". Pero muchos usuarios y grandes comunidades de desarrollo "auto-soportan" estos paquetes.

Ningún fabricante de software carece de su propia oferta. Es una realidad indiscutible.

En los capítulos previos ya hemos discutido acerca de ejemplos en países como Japón, Europa, US, India y Australia.

Necesitaremos mirar, una y otra vez, muy seriamente, a lo largo del Año 2000. ¡No es un mito!

2. ¿Cuándo debo migrar a IPv6?

Muchos de nosotros ya hemos empezado, de alguna manera, probablemente a través de túneles.
Necesitamos forzar la creación de plataformas de prueba, y usar IPv6 a través de Internet con otros usuarios IPv6.
Las compañías comerciales, en la mayoría de las ocasiones, esperarán hasta que la normalización sea completa y clara, y puedan evaluar adecuadamente los costes, etc.

Pero para redes sin ánimo de lucro, como investigación, educación, deben migrar gradualmente ahora, logrando experiencia y compartiéndola con otros. Después de todo, las redes de I+D siempre son las primeras en comenzar trabajando con todo, como así fue con Internet.

Conclusión: tan pronto como sea posible, dependiendo de su caso. Puede que cuando piense que va a necesitar más direcciones IP, ya sea demasiado tarde.

3. Recursos de IPv6

Para finalizar con esta introducción, recopilamos una breve relación de URL's donde el lector puede continuar aprendiendo acerca de IPv6:

- Foro IPv6: http://www.ipv6forum.com/
- Página de información IPv6: http://www.ipv6.org/
- IPv6 Over Everything: http://www.data.com/issue/991021/ipv6.html
- Why IPv6?: http://www.opengroup.org/orc/xnet/yv6/
- IPng: http://playground.sun.com/pub/ipng/html/
- IETF IPng Working Group: http://playground.sun.com/pub/ipng/html/meetings.html
- The 6Bone Network: http://www.6bone.net/
- Internet2: http://www.internet2.org/
- IAB: http://128.9.160.55/

Esta relación es una lista muy limitada de los recursos disponibles en la Web. Pero es un punto por donde empezar.
En muchos de estos sitios, podrá encontrar hiperenlaces a mucha información adicional. Si eso no le es suficiente, seguro que le bastará con apuntar su herramienta de búsqueda favorita y preguntar por "IPv6". Probablemente, ¡no tendrá tiempo suficiente para leer todo lo que pueda localizar!
Listas de correo relacionadas con IPv6:

- users@ipv6.org
- education@ipv6forum.com
- deployment@ipv6.org
- projects@ipv6forum.com
- tech@ipv6forum.com
- ipng@sunroof.eng.sun.com

Bibliografía

[RFC791] RFC 791: "Internet Protocol"
Jon Postel
Septiembre 1.981

[RFC792] RFC 792: "Internet Control Message Protocol"
Jon Postel
Septiembre 1.981

[RFC801] RFC801: "NCP/TCP TRANSITION PLAN"
Jon Postel
Noviembre 1.981

[RFC907] RFC907: "INTERNET SUBNETS"
Jeffrey Mogul
Octubre 1.984

[RFC919] RFC919: "BROADCASTING INTERNET DATAGRAMS"
Jeffrey Mogul
Octubre 1.994

[RFC922] RFC922: "BROADCASTING INTERNET DATAGRAMS IN THE
PRESENCE OF SUBNETS"
Jeffrey Mogul
Octubre 1.984

[RFC925] RFC925: "Multi-LAN Address Resolution"
Jon Postel
Octubre 1.984

[RFC932] RFC932: "A SUBNETWORK ADDRESSING SCHEME"
David D. Clark
Enero 1.985

[RFC936] RFC936: "Another Internet Subnet Addressing Scheme"
Michael J. Karels
Febrero 1.985

[RFC940] RFC940: "Toward an Internet Standard Scheme for Subnetting"
Gateway Algorithms and Data Structures (GADS) Task Force
Abril 1.985

[RFC947] RFC947: "Multi-network Broadcasting within the Internet"
Ken Lebowitz
David Mankins
Junio 1.985

[RFC950] RFC950: "Internet Standard Subnetting Procedure"
J. Mogul
Jon Postel
Agosto 1.985

[RFC966] RFC966: "Host Groups: A Multicast Extension to the Internet Protocol"
S. E. Deering
D. R. Cheriton
Diciembre 1.985

[RFC988] RFC988: "Host Extensions for IP Multicasting"
S. E. Deering
Julio 1.986

[RFC1108] RFC1108: "U.S. Department of Defense Security Options for the Internet Protocol"
Stephen Kent
Noviembre 1.991

[RFC1112] RFC1112: "Host Extensions for IP Multicasting"
Steve Deering
Agosto 1.989

[RFC1191] RFC1191: "Path MTU Discovery"
Jeffrey Mogul
Steve Deering
Noviembre 1.990

[RFC1234] RFC1234: "Tunneling IPX Traffic through IP Networks"
Don Provan
Junio 1.991

[RFC1241] RFC1241: "A Scheme for an Internet Encapsulation Protocol: Version 1"
Robert A. Woodburn
David L. Mills
Julio 1.991

[RFC1272] RFC1272: "INTERNET ACCOUNTING: BACKGROUND"
Cyndi Mills
Donald Hirsh

Gregory Ruth
Noviembre 1.991

[RFC1281] RFC1281: "Guidelines for the Secure Operation of the Internet"
Richard D. Pethia
Stephen D. Crocker
Barbara Y. Fraser
Noviembre 1.991

[RFC1287] RFC1287: "Towards the Future Internet Architecture"
David D. Clark
Vinton G. Cerf
Lyman A. Chapin
Robert Braden
Russell Hobby
Diciembre 1.991

[RFC1335] RFC1335: "A Two-Tier Address Structure for the Internet: A Solution to the Problem of Address Space Exhaustion"
Zheng Wang
Jon Crowcroft
Mayo 1.992

[RFC1338] RFC1338: "Supernetting: an Address Assignment and Aggregation Strategy"
Vince Fuller
Tony Li
Jessica (Jie Yun) Yu
Kannan Varadhan
Junio 1.992

[RFC1347] RFC1347: "TCP and UDP with Bigger Addresses (TUBA), A
Simple Proposal for Internet Addressing and Routing"
Ross Callon
Junio 1.992

[RFC1349] RFC1349: "Type of Service in the Internet Protocol Suite"
Philip Almquist
Julio 1.992

[RFC1380] RFC1380: "IESG Deliberations on Routing and Addressing"
Phillip Gross
Philip Almquist

Noviembre 1.992

[RFC1393] RFC1393: "Traceroute Using an IP Option"
Gary Scott Malkin
Enero 1.993

[RFC1435] RFC1435: "IESG Advice from Experience with Path MTU Discovery"
Stev Knowles
Marzo 1.993

[RFC1454] RFC1454: "Comparison of Proposals for Next Version of IP"
Tim Dixon
Mayo 1.993

[RFC1455] RFC1455: "Physical Link Security Type of Service"
Donald E. Eastlake, III
Mayo 1.993

[RFC1466] RFC1466: "Guidelines for Management of IP Address Space"
Elise Gerich
Mayo 1.993

[RFC1467] RFC1467: "Status of CIDR Deployment in the Internet"
Claudio Topolcic
Agosto 1.993

[RFC1475] RFC1475: "TP/IX: The Next Internet"
Robert Ullmann
Junio 1.993

[RFC1481] RFC1481: "IAB Recommendation for an Intermediate Strategy to Address the Issue of Scaling"
Christian Huitema
Julio 1.993

[RFC1517] RFC1517: "Applicability Statement for the Implementation of Classless Inter-Domain Routing (CIDR)"
Robert M. Hinden
Septiembre 1.993

[RFC1518] RFC1518: "An Architecture for IP Address Allocation with CIDR"
Yakov Rekhter
Tony Li

Septiembre 1.993

[RFC1519] RFC1519: "Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy"
Vince Fuller
Tony Li
Septiembre 1.993

[RFC1520] RFC1520: "Exchanging Routing Information Across Provider Boundaries in the CIDR Environment"
Yakov Rekhter
Claudio Topolcic
Septiembre 1.993

[RFC1526] RFC1526: "Assignment of System Identifiers for TUBA/CLNP Hosts"
David M. Piscitello
Septiembre 1.993

[RFC1541] RFC1541: "Dynamic Host Configuration Protocol"
R. Droms
Octubre 1993

[RFC1546] RFC1546: "Host Anycasting Service"
Walter Milliken
Trevor Mendez
Craig Partridge
Noviembre 1.993

[RFC1550] RFC1550: "IP: Next Generation (IPng) White Paper Solicitation"
Scott Bradner
Allison Mankin
Diciembre 1.993

[RFC1560] RFC1560: "The MultiProtocol Internet"
Dr. Barry M. Leiner
Yakov Rekhter
Diciembre 1.993

[RFC1597] RFC1597: "Address Allocation for Private Internets"
Yakov Rekhter
Robert G Moskowitz
Daniel Karrenberg
Geert Jan de Groot
Marzo 1.994

[RFC1621] RFC1621: "Pip Near-term Architecture"

Paul Francis
Mayo 1.994

[RFC1622] RFC1622: "Pip Header Processing"
Paul Francis
Mayo 1.994

[RFC1636] RFC1636: "Report of IAB Workshop on Security in the Internet Architecture. February 8-10, 1994"
Bob Braden
David Clark
Steve Crocker
Christian Huitema
Junio 1.994

[RFC1639] RFC1639: "FTP Operation Over Big Address Records (FOOBAR)"
David M. Piscitello
Junio 1.994

[RFC1667] RFC1667: "Modeling and Simulation Requirements for IPng"
Susan Symington
David Wood
J. Mark Pullen
Agosto 1.994

[RFC1668] RFC1668: "Unified Routing Requirements for IPng"
Deborah Estrin
Tony Li
Yakov Rekhter
Agosto 1.994

[RFC1669] RFC1669: "Market Viability as a IPng Criteria"
John Curran
Agosto 1.994

[RFC1670] RFC1670: "Input to IPng Engineering Considerations"
Denise Heagerty
Agosto 1.994

[RFC1671] RFC1671: "IPng White Paper on Transition and Other Considerations"
Brian E. Carpenter
Agosto 1.994

[RFC1672] RFC1672: "Accounting Requirements for IPng"
Nevil Brownlee

Agosto 1.994

[RFC1673] RFC1673: "Electric Power Research Institute Comments on IPng"
Ron Skelton
Agosto 1.994

[RFC1674] RFC1674: "A Cellular Industry View of IPng"
Mark S. Taylor
Agosto 1.994

[RFC1675] RFC1675: "Security Concerns for IPng"
Steven M. Bellovin
Agosto 1.994

[RFC1676] RFC1676: "INFN Requirements for an IPng"
Davide Salomoni
Cristina Vistoli
Antonia Ghiselli
Agosto 1.994

[RFC1677] RFC1677: "Tactical Radio Frequency Communication Requirments for IPng"
R. Brian Adamson
Agosto 1.994

[RFC1678] RFC1678: "IPng Requirements of Large Corporate Networks"
Edward Britton
John Tavs
Agosto 1.994

[RFC1679] RFC1679: "HPN Working Group Input to the IPng Requirements Solicitation"
Dan Green
Phil Irey
Dave Marlow
Karen O'Donoghue
Agosto 1.994

[RFC1680] RFC1680: "IPng Support for ATM Services"
Christina Brazdziunas
Agosto 1.994

[RFC1681] RFC1681: "On Many Addresses per Host"
Steven M. Bellovin
Agosto 1.994

[RFC1682] RFC1682: "IPng BSD Host Implementation Analysis"
Jim Bound
Agosto 1.994

[RFC1683] RFC1683: "Multiprotocol Interoperability In IPng"
Russell J. Clark
Mostafa H. Ammar
Kenneth L. Calvert
Agosto 1.994

[RFC1686] RFC1686: "IPng Requirements: A Cable Television Industry Viewpoint"
Mario P. Vecchi
Agosto 1.994

[RFC1687] RFC1687: "A Large Corporate User's View of IPng"
Eric Fleischman
Agosto 1.994

[RFC1688] RFC1688: "IPng Mobility Considerations"
William Allen Simpson
Agosto 1.994

[RFC1701] RFC1701: "Generic Routing Encapsulation (GRE)"
Stan Hanks
Tony Li
Dino Farinacci
Paul Traina
Octubre 1.994

[RFC1705] RFC1705: "Six Virtual Inches to the Left: The Problem with IPng"
Richard Carlson
Domenic Ficarella
Octubre 1.994

[RFC1707] RFC1707: "CATNIP: Common Architecture for the Internet"
Michael McGovern
Robert Ullmann
Octubre 1.994

[RFC1710] RFC1710: "Simple Internet Protocol Plus White Paper"
Robert M. Hinden
Octubre 1.994

[RFC1719] RFC1719: "A Direction for IPng"
Phill Gross

Diciembre 1.994

[RFC1726] RFC1726: "Technical Criteria for Choosing IP The Next Generation (IPng)"
Craig Partridge
Frank Kastenholz
Diciembre 1.994

[RFC1750] RFC1750: "Randomness Recommendations for Security"
Donald E. Eastlake 3rd
Stephen D. Crocker
Jeffrey I. Schiller
Diciembre 1.994

[RFC1752] RFC1752: "The Recommendation for the IP Next Generation Protocol"
Scott Bradner
Allison Mankin
Enero 1.995

[RFC1753] RFC1753: "IPng Technical Requirements Of the Nimrod Routing and Addressing Architecture"
J. Noel Chiappa
Enero 1.995

[RFC1797] RFC1797: "Class A Subnet Experiment"
Internet Assigned Numbers Authority (IANA)
Abril 1.995

[RFC1809] RFC1809: "Using the Flow Label Field in IPv6"
Craig Partridge
Junio 1.995

[RFC1817] RFC1817: "CIDR and Classful Routing"
Yakov Rekhter
Agosto 1.995

[RFC1825] RFC1825: "Security Architecture for the Internet Protocol"
Randall Atkinson
Agosto 1.995

[RFC1826] RFC1826: "IP Authentication Header"
Randall Atkinson
Agosto 1.995

[RFC1827] RFC1827: "IP Encapsulating Security Payload (ESP)"
Randall Atkinson

Agosto 1.995

[RFC1828] RFC1828: "IP Authentication using Keyed MD5"
Perry Metzger
William Allen Simpson
Agosto 1.995

[RFC1829] RFC1829: "The ESP DES-CBC Transform"
Perry Metzger
William Allen Simpson
Agosto 1.995

[RFC1852] RFC1852: "IP Authentication using Keyed SHA"
Perry Metzger
William Allen Simpson
Septiembre 1.995

[RFC1853] RFC1853: "IP in IP Tunneling"
William Allen Simpson
Octubre 1.995

[RFC1878] RFC1878: "Variable Length Subnet Table For IPv4"
Troy T. Pummill
Bill Manning
Diciembre 1.995

[RFC1879] RFC1879: "Class A Subnet Experiment Results and Recommendations"
Bill Manning
Enero 1.996

[RFC1881] RFC1881: "IPv6 Address Allocation Management"
Internet Architecture Board
Internet Engineering Steering Group
Diciembre 1.995

[RFC1883] RFC1883: "Internet Protocol, Version 6 (IPv6) Specification"
Stephen E. Deering
Robert M. Hinden
Diciembre 1.995

[RFC1884] RFC1884: "IP Version 6 Addressing Architecture"
Robert M. Hinden
Stephen E. Deering
Diciembre 1.995

[RFC1885] RFC1885: "Internet Control Message Protocol (ICMPv6)

for the Internet Protocol Version 6 (IPv6)
Specification"
Stephen Deering
Alex Conta
Diciembre 1.995

[RFC1886] RFC1886: "DNS Extensions to support IP version 6"
Susan Thomson
Christian Huitema
Diciembre 1.995

[RFC1887] RFC1887: "An Architecture for IPv6 Unicast Address Allocation"
Yakov Rekhter
Tony Li
Diciembre 1.995

[RFC1897] RFC1897: "IPv6 Testing Address Allocation"
Robert M. Hinden
Jon Postel
Enero 1.996

[RFC1917] RFC1917: "An Appeal to the Internet Community to Return Unused IP Networks (Prefixes) to the IANA"
Philip J. Nesser II
Febrero 1.996

[RFC1924] RFC1924: "A Compact Representation of IPv6 Addresses"
Robert Elz
Abril 1.996

[RFC1933] RFC1933: "Transition Mechanisms for IPv6 Hosts and Routers"
Robert E. Gilligan
Erik Nordmark
Abril 1.996