



Universidad de San Carlos de Guatemala  
Facultad de Ingeniería  
Escuela de Ingeniería Mecánica Eléctrica

## **MIGRACIÓN DEL PROTOCOLO IPv4 A IPv6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO**

**Edwin Felipe Morales Cal**  
**Asesorado por el Ing. Julio César Solares Peñate**

Guatemala, agosto de 2009

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA



FACULTAD DE INGENIERÍA

**MIGRACIÓN DEL PROTOCOLO IPv4 A IPv6 EN UNA RED, LOS BENEFICIOS  
Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO**

TRABAJO DE GRADUACIÓN

PRESENTADO A JUNTA DIRECTIVA DE LA  
FACULTAD DE INGENIERÍA  
POR

**EDWIN FELIPE MORALES CAL**

ASESORADO POR EL INGENIERO JULIO CÉSAR SOLARES PEÑATE

AL CONFERÍRSELE EL TÍTULO DE  
**INGENIERO ELECTRÓNICO**

GUATEMALA, AGOSTO DE 2009

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA



### **NÓMINA DE JUNTA DIRECTIVA**

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Angel Dávila Calderón
VOCAL IV	Br. José Milton De León Bran
VOCAL V	Br. Isaac Sultán Mejía
SECRETARIA	Inga. Marcia Ivónne Véliz Vargas

### **TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO**

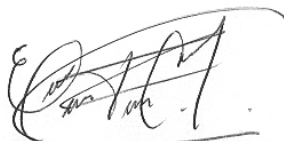
DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Julio César Solares Peñate
EXAMINADOR	Ing. Marvin Marino Hernández Fernández
EXAMINADOR	Inga. Ingrid Salomé Rodríguez de Loukota
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

## **HONORABLE TRIBUNAL EXAMINADOR**

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

**MIGRACIÓN DEL PROTOCOLO IPv4 A IPv6 EN UNA RED,  
LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE  
CAMBIO,**

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, en mayo de 2003.



**Edwin Felipe Morales Cal**

Guatemala, 17 de julio de 2009

Señor Coordinador de Electrónica  
Escuela de Ingeniería Mecánica Eléctrica  
Facultad de Ingeniería, USAC.

Señor Coordinador:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **"MIGRACION DEL PROTOCOLO IPV4 A IPV6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO"**, desarrollado por el estudiante **Edwin Felipe Morales Cal**, ya que considero que cumple con los requisitos establecidos.

Por lo tanto, el autor de este trabajo y yo como asesor, nos hacemos responsables del contenido y conclusiones del mismo.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

  
Ing. Julio César Solares Peñate  
**ASESOR**



**FACULTAD DE INGENIERIA**

Escuelas de Ingeniería Civil, Ingeniería  
Mecánica Industrial, Ingeniería Química,  
Ingeniería Mecánica Eléctrica, Técnica  
y Regional de Post-grado de Ingeniería  
Sanitaria.

Ciudad Universitaria, zona 12  
Guatemala, Centroamérica

Guatemala, 3 de agosto de 2009

Señor Director  
Ing. Mario Renato Escobedo Martínez  
Escuela de Ingeniería Mecánica Eléctrica  
Facultad de Ingeniería, USAC.

Señor Director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **“MIGRACION DEL PROTOCOLO IPV4 A IPV6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO”**, desarrollado por el estudiante **Edwin Felipe Morales Cal**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

**ID Y ENSEÑAD A TODOS**

  
Ing. Julio César Solares Peñate  
Coordinador de Electrónica



UNIVERSIDAD DE SAN CARLOS  
DE GUATEMALA



FACULTAD DE INGENIERIA

REF. EIME 46. 2009.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; Edwin Felipe Morales Cal titulado: "MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO", procede a la autorización del mismo.

Ing. Mario Renato Espinosa Martínez



GUATEMALA, 10 DE AGOSTO 2,009.

Universidad de San Carlos  
de Guatemala



Facultad de Ingeniería  
Decanato

Ref. DTG.312.2009

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **MIGRACIÓN DEL PROTOCOLO IPV4 A IPV6 EN UNA RED, LOS BENEFICIOS Y SEGURIDAD QUE CONLLEVA ESTE CAMBIO**, presentado por el estudiante universitario **Edwin Felipe Morales Cal**, autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Murphy Olimpo Paiz Recinos  
DECANO



Guatemala, agosto de 2009

/cc



## **DEDICATORIA A:**

### **DIOS**

Por darme la vida, estar siempre presente en ella y por la bendición de poder alcanzar este logro

### **MI PADRE**

Felipe Morales Guatzín, por brindarme su ejemplo de superación, trabajo y dedicación, además por el esfuerzo y apoyo incondicional que me brindó durante mi trayectoria académica

### **MI MADRE**

Rosa María Cal de Morales, por todo el amor que me brinda, por su comprensión, ternura, tiempo, cariño y por estar siempre a mi lado para apoyarme y enseñarme el camino correcto

### **MI HERMANO**

Otto Fernando Morales Cal, por mostrarme el camino académico que tomé y por sus consejos que durante este tiempo me sirvieron de mucho

### **MIS FAMILIARES**

Por ser parte esencial de mi vida, por estar presentes en todo momento y por preocuparse de mi persona

## **AGRADECIMIENTOS A:**

### **DIOS**

Porque gracias a Él, obtengo este logro y sé que junto a Él alcanzaré muchos más

### **MIS PADRES**

Por existir en mi vida, por sus consejos y por haberme brindado la oportunidad de prepararme académicamente

### **MIS CATEDRÁTICOS**

Quienes me transmitieron todo su valioso conocimiento y me brindaron las herramientas necesarias para poder desarrollarme, tanto laboral como académicamente

### **MIS COMPAÑEROS DE ESTUDIO**

Por brindarme su invaluable amistad, el apoyo mutuo que nos brindamos y por seguir siendo amigos

### **MIS COMPAÑEROS DE TRABAJO**

Por compartirme todo su conocimiento y brindarme su amistad y confianza. Así como por su influencia para poder alcanzar este grado académico

**MIS AMIGOS**

**Y AMIGAS**

Por estar presentes en mi vida, por su amistad incondicional, por los buenos momentos que vivimos y que seguiremos viviendo.

**LA UNIVERSIDAD SAN**

**CARLOS DE GUATEMALA**

Por ser la casa de estudios que me preparara profesionalmente y ello me permitiera poder contribuir en la mejora de nuestra bella Guatemala.

## ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES	VII
LISTA DE ABREVIATURAS	XI
GLOSARIO	XV
RESUMEN	XIX
OBJETIVOS	XXI
INTRODUCCIÓN	XXIII
<b>1. INTRODUCCIÓN A LAS REDES</b>	<b>1</b>
1.1. Redes de computadoras	1
1.1.1. Clasificación según distribución de área geográfica	4
1.1.1.1. Red de área local	4
1.1.1.2. Red de área metropolitana	6
1.1.1.3. Red de área extensa	7
1.1.1.4. Red de área de almacenamiento	11
1.1.2. Topología de red	12
1.1.2.1. Topologías físicas de LAN	13
1.1.2.1.1. Topología en bus y árbol	13
1.1.2.1.2. Topología en anillo	16
1.1.2.1.3. Topología en estrella	19
1.1.2.2. Topologías lógicas	20
1.1.2.2.1. No determinísticas	21
1.1.2.2.1.1. Ethernet	21
1.1.2.2.1.2. Fastethernet	32
1.1.2.2.1.3. Gigabitethernet	33
1.1.2.2.2. Determinísticas	38

1.1.2.2.2.1. Token ring	38
1.1.2.2.2.2. FDDI	43
<b>2. ANÁLISIS DEL PROTOCOLO ACTUAL IPv4</b>	<b>49</b>
2.1. Modelo de referencia OSI	49
2.2. Modelo TCP/IP	56
2.3. Principales protocolos del conjunto TCP/IP	61
2.4. Características de IP versión 4	63
2.4.1. ICMPv4	70
2.4.2. IGMPv4	76
2.5. Direccionamiento IP en versión 4	78
2.5.1. Formato de una dirección IPv4	79
2.5.2. Clases de direcciones en IPv4	80
2.5.3. Direcciones IP privadas y públicas	82
2.5.4. División de redes en subredes	85
2.6. Enrutamiento y transporte	87
2.6.1. Protocolos de enrutamiento dinámico	88
2.6.1.1. IGP's	89
2.6.1.2. EGP's	92
2.7. Seguridad necesaria en IPv4	94
2.7.1. Criptografía y sus algoritmos	95
2.7.2. Protección de una red utilizando un contra-fuegos	97
2.8. IPv4 limitaciones a corto plazo	98
<b>3. IPv6 LA SIGUIENTE GENERACIÓN</b>	<b>101</b>
3.1. Distribución de recursos en Internet	101
3.2. ¿Por qué cambiar a un nuevo protocolo de Internet?	102
3.3. Características y beneficios de IPv6	109
3.4. Formato de la cabecera IPv6	110

3.4.1.	Campos de la cabecera IPv6	112
3.4.2.	Extensiones de la cabecera IPv6	114
3.4.2.1.	Salto a salto	117
3.4.2.2.	Enrutamiento	118
3.4.2.3.	Fragmento	120
3.4.2.4.	Opciones de destino	122
3.4.2.5.	Autenticación y seguridad del encapsulado de carga útil	123
3.4.2.6.	Sin siguiente cabecera	123
3.5.	Tamaño del datagrama en IPv6	124
3.5.1.	Descubrimiento de la MTU de la ruta	124
3.6.	Direccionamiento en IP versión 6	126
3.6.1.	Algunas reglas generales de las direcciones IPv6	127
3.6.2.	Formato de las direcciones en IPv6	128
3.6.2.1.	Representación textual de las direcciones	128
3.6.2.2.	Representación textual de los prefijos	130
3.6.3.	Identificación del tipo de dirección	131
3.6.4.	Direcciones Unicast en IPv6	132
3.6.4.1.	Identificadores de interface	132
3.6.4.2.	Direcciones sin especificar	133
3.6.4.3.	Direcciones Loopback	133
3.6.4.4.	Direcciones globales Unicast	133
3.6.4.5.	Direcciones IPv6 con direcciones IPv4 insertadas	135
3.6.4.6.	Direcciones Unicast IPv6 de enlace-local	136
3.6.5.	Direcciones Anycast en IPv6	137
3.6.6.	Direcciones Multicast en IPv6	137
3.7.	Enrutamiento en IPv6	139
3.7.1.	Rutas estáticas	140
3.7.2.	RIP	141

3.7.3. OSPF	142
3.7.4. IS-IS	143
3.7.5. BGP	144
<b>4. ESTRATEGIA DE MIGRACIÓN A IPv6 Y SEGURIDAD QUE CONLLEVA</b>	<b>147</b>
4.1. Seguridad que conlleva la migración a IPv6	147
4.1.1. IPsec	149
4.1.1.1. Asociaciones de seguridad	150
4.1.1.2. Cabecera de autenticación AH	150
4.1.1.3. Cabecera ESP	153
4.2. Mecanismos de migración a IPv6	156
4.2.1. Doble pila	157
4.2.2. Túneles IPv6 sobre IPv4	158
4.2.2.1. Encapsulamiento	159
4.2.2.2. Túnel automático	160
4.2.2.3. Túnel manual	161
4.2.2.4. 6to4	161
4.2.2.5. ISATAP	165
4.2.2.6. TSP negociador de túneles	167
4.2.2.7. Teredo	170
4.2.2.8. GRE soportando IPv6	172
4.3. Configuraciones necesarias para la migración a IPv6	172
4.3.1. Configuración de interfaces y avisos de enrutadores	173
4.3.2. Gestión de vecinos en host y enrutadores	176
4.3.3. Gestión de mensajes ICMP en host y enrutadores	177
4.3.4. Configuración estática de un servidor DNS	177
4.3.5. Configuración de enrutamiento	178
4.3.5.1. Rutas estáticas	179

4.3.5.2. IPv6 forwarding / CEF	180
4.3.5.3. RIP	181
4.3.5.4. OSPF	182
4.3.5.5. IS-IS	183
4.3.5.6. BGP	184
4.3.6. Configuración de túneles	186
4.3.6.1. Túnel estático	186
4.3.6.2. 6to4	187
4.3.6.3. ISATAP	189
4.3.6.4. TSP negociador de túneles	190
4.3.6.5. GRE soportando IPv6	191
CONCLUSIONES	193
RECOMENDACIONES	195
BIBLIOGRAFÍA	197





## ÍNDICE DE ILUSTRACIONES

### FIGURAS

1	Modelo cliente-servidor	2
2	Modelo igual-igual	3
3	Ejemplo de red de área local	5
4	Ejemplo de red de área metropolitana	6
5	Ejemplo de red de área extensa conexión a internet	8
6	Ejemplo de WAN agencias bancarias	9
7	Ejemplo de red de área de almacenamiento	12
8	Ejemplo de topología física en bus	14
9	Ejemplo de topología física en árbol	16
10	Ejemplo de topología física en anillo	17
11	Ejemplo de topología en estrella	19
12	Estructura de la trama genérica Ethernet	24
13	Estructura de la trama IEEE 802.3	25
14	Especificación de norma según medio utilizado	30
15	Red Gigabit ethernet utilizando conmutadores	34
16	Funcionamiento de token ring	39
17	Formato de una trama token ring	40
18	Detalle de los campos de una trama token ring	41
19	Ejemplo de una red utilizando topología FDDI	43
20	Formato de una trama genérica FDDI y de un testigo	45
21	Ejemplo del funcionamiento de una red con FDDI	47
22	Capas del modelo de referencia OSI	50
23	Subdivisión de la capa de enlace de datos	52

24	Proceso de comunicación entre dos estaciones	56
25	Capas del modelo TCP/IP	57
26	Comparación entre OSI y TCP/IP	60
27	Arquitectura de protocolos de TCP/IP	61
28	Formato de la cabecera de un paquete IP versión 4	64
29	Formato del campo TOS	65
30	Formato de la opción seguridad en IPv4	69
31	Formato de un mensaje ICMPv4	72
32	Formato de un mensaje ICMP de eco	74
33	Formato de un mensaje ICMP de destino inalcanzable	74
34	Formato de un mensaje IGMP de destino inalcanzable	77
35	Clases de direcciones IPv4	80
36	Organigrama para la distribución de recursos de Internet	102
37	Estado a fecha 03/05/09 del espacio de direcciones IPv4	104
38	Desglose de direcciones asignadas por IANA a RIRs	105
39	Estado de direcciones IP de acuerdo con conjunto de estados	106
40	Estado de direcciones IP categorizada por RIR	107
41	Cabecera básica IPv6	111
42	Cabecera de enrutamiento	118
43	Cabecera Fragmento	120
44	Paquete original y fragmentos	121
45	Cabecera Opciones de destino	122
46	Proceso de descubrimiento de MTU	125
47	Formato general de una dirección IPv6	127
48	Formato básico de una dirección global Unicast	134
49	Formato de una dirección IPv4 compatible con IPv6	135
50	Formato de una dirección IPv4 direccionada como IPv6	136
51	Formato de una dirección Unicast IPv6 de enlace local	136
52	Formato de una dirección Multicast	138

53	Campos del datagrama IP protegidos por AH de IPsec	151
54	Formato de cabecera AH	152
55	Formato de la cabecera ESP	154
56	Encapsulamiento de un datagrama IPv6	159
57	Estructura de la dirección 6to4	163
58	Esquema del mecanismo 6to4	164
59	Formato de la dirección ISATAP	166
60	Modelo del mecanismo tunnel broker	168
61	Modelo del mecanismo Teredo	170
62	Formato de la dirección Teredo	171
63	Ejemplo de túnel estático	186
64	Ejemplo de 6to4	188
65	Ejemplo de ISATAP	189
66	Ejemplo de un cliente TSP tunnel broker	190

## TABLAS

I	Disposición de pines en un conector RJ-45	31
II	Versiones de Gigabit Ethernet según el medio de transmisión	36
III	Tipos de opciones del datagrama IPv4	68
IV	Tipos de mensajes ICMPv4	72
V	Tipos de códigos ICMPv4 de destino inalcanzable	75
VI	Direcciones privadas	84
VII	Máscaras por defecto	85
VIII	Atributos de BGP	93
IX	Valores de siguiente cabecera para las extensiones IPv6	115
X	Orden de las extensiones de cabecera IPv6	116
XI	Identificación del tipo de dirección IPv6	131
XII	Valores del campo alcance	139



## LISTA DE ABREVIATURAS

<b>AH</b>	Authentication header (cabecera de autenticación)
<b>API</b>	Application Programming Interface (Interfaz de programación de aplicaciones)
<b>ARP</b>	Address Resolution Protocol (protocolo de resolución de direcciones)
<b>ARPANET</b>	Advanced Research Projects Agency Network (Red de la agencia de proyectos de investigación avanzada)
<b>AS</b>	Autonomous System (Sistema autónomo)
<b>ATM</b>	Asynchronous Transfer Mode (Modo de transferencia asíncrono)
<b>BGP</b>	Border Gateway Protocol (Protocolo de Gateway fronterizo)
<b>CIDR</b>	Classless Interdomain Routing (Enrutamiento entre dominios sin clase)
<b>CSMA/CD</b>	Carrier Sense Multiple Access / Collision Detect (Acceso múltiple con detección de portadora y detección de colisiones)

<b>CRC</b>	Cyclic Redundancy Check (Verificación por redundancia crítica)
<b>CSU</b>	Channel Service Unit (Unidad de servicio de canal)
<b>DSL</b>	Digital Subscriber Line (Línea de abonado digital)
<b>DSU</b>	Data Service Unit (Unidad de servicio de datos)
<b>EIA</b>	Electronic Industries Association (Asociación de industrias electrónicas)
<b>FDDI</b>	Fiber Distributed Data Interface (Interfaz de datos distribuidos por fibra)
<b>HTTP</b>	Hypertext Transfer Protocol (Protocolo de transferencia de hipertexto)
<b>IANA</b>	Internet Assigned Numbers Authority (Agencia de asignación de números de Internet)
<b>ICMP</b>	Internet Control Message Protocol (Protocolo de mensajes de control en Internet)
<b>IETF</b>	Internet Engineering Task Force (Grupo de Ingeniería de Internet)

<b>IGMP</b>	Internet Group Management Protocol (Protocolo de administración de grupos de Internet)
<b>IGP</b>	Interior Gateway Protocol (Protocolo de Gateway interior)
<b>IP</b>	Internet Protocol (Protocolo Internet)
<b>IS-IS</b>	Intermediate System to Intermediate System Protocol (Sistema intermedio a sistema intermedio)
<b>ISO</b>	International Organization for Standardization (Organización internacional para la normalización)
<b>ISP</b>	Internet Service Provider (Proveedor de servicios de Internet)
<b>MAC</b>	Media Access Control (Control de acceso al medio)
<b>MTU</b>	Maximum Transmission Unit (Unidad máxima de transmisión)
<b>NIC</b>	Network Interface Card (Tarjeta de interfaz de red)
<b>OSI</b>	Open Systems Interconnection (Interconexión de sistemas abiertos)
<b>OSPF</b>	Open Shortest Path First (Primer camino abierto más corto)



<b>PDU</b>	Protocol Data Unit (Unidad de datos del protocolo)
<b>QoS</b>	Quality of Service (Calidad de servicio)
<b>RFC</b>	Request for Comments (Petición de comentarios)
<b>SNMP</b>	Simple Network Management Protocol (Protocolo simple de administración de redes)
<b>SONET</b>	Synchronous Optical Network (Red óptica síncrona)
<b>TCP/IP</b>	Transmission Control Protocol / Internet Protocol (Protocolo para el control de la transmisión / Protocolo Internet)
<b>UDP</b>	User Datagram Protocol (Protocolo de datagrama de usuario)

## GLOSARIO

<b>Autenticación</b>	La verificación de la identidad de una persona o proceso.
<b>Ancho de banda</b>	Diferencia entre las frecuencias más altas y más bajas disponibles para las señales de red.
<b>Banda base</b>	Característica de una tecnología de red donde sólo se utiliza una frecuencia portadora.
<b>Binario</b>	Sistema numérico compuesto por unos y ceros.
<b>Bit de relleno</b>	La inserción de bits extra en una cadena de datos para evitar la aparición de secuencias de control no deseadas.
<b>Broadcast</b>	Paquete de datos enviado a todos los nodos de una red. Las difusiones se identifican por una dirección de difusión.
<b>Cabecera</b>	Información de control de un sistema definido que precede a los datos del usuario.
<b>Capa</b>	Grupo de servicios, funciones y protocolos que se definen totalmente desde un punto de vista conceptual, que constituye uno de entre un conjunto de grupos dispuestos jerárquicamente, y que se extiende a través de todos los sistemas que conforman la arquitectura de la red.

<b>Colisión</b>	En Ethernet, el resultado de dos nodos que transmiten simultáneamente.
<b>Criptografía</b>	Técnica que permite cifrar los mensajes antes de su transmisión.
<b>Datagrama</b>	Agrupamiento lógico de información enviada como unidad de capa de red a través de un medio de transmisión sin establecer previamente un circuito virtual.
<b>Enrutamiento</b>	Determinación del camino o ruta que las unidades de datos (tramas, paquetes, mensajes) atravesarán desde la fuente al destino.
<b>Encapsulado</b>	Adición de información de control mediante una entidad de protocolo con datos obtenidos de un protocolo de usuario.
<b>Host</b>	Computadora de una red. Similar a nodo, salvo que el host normalmente implica una computadora, mientras nodo generalmente se aplica a cualquier sistema de red, incluyendo servidores y routers.
<b>Hub</b>	Dispositivo que sirve como centro de una topología en estrella. También denominado repetidor multipuerto.
<b>Integridad</b>	Resistencia al cambio por errores del sistema.
<b>Interface</b>	Conexión entre dos sistemas o dispositivos. En terminología de enrutamiento es una conexión de red

<b>Internet</b>	Abreviatura de internetwork, la cual es un conjunto de redes interconectadas mediante routers y otros dispositivos, que funciona generalmente como una red.
<b>InterNIC</b>	Organización que ofrece asistencia al usuario, documentación, capacitación, servicios de registro para nombres de dominio de Internet, direcciones de red y otros servicios a la comunidad de Internet.
<b>IP</b>	Protocolo de capa de red de la pila TCP/IP que ofrece un servicio de internetwork no orientado a conexión.
<b>IPsec</b>	Conjunto de medidas de seguridad para proteger las transmisiones del protocolo IP.
<b>Enlace</b>	Canal de comunicaciones de red que se compone de un circuito o ruta de transmisión y todo el equipo relacionado entre un emisor y un receptor.
<b>Nodo</b>	Punto final de la conexión de red o una unión que es común para dos o más líneas de una red. Pueden ser procesadores, controladores o estaciones de trabajo.
<b>Paquete</b>	Grupo de bits que incluyen datos e información adicional de control. Generalmente se refiere a una unidad de datos del protocolo de la capa de red.
<b>Ping</b>	Comando que utiliza el protocolo ICMP para verificar la conexión de hardware y la dirección lógica de la capa de

red. Es un mecanismo de prueba muy básico que se usa en redes IP para probar el alcance de un dispositivo de red.

<b>Protocolo</b>	Descripción formal de un conjunto de reglas y convenciones que determinan la forma en la que los dispositivos de una red intercambian información
<b>Router</b>	Dispositivo de capa de red que utiliza una o más métricas para determinar la ruta óptima por la cual se enviará el tráfico de la red.
<b>Topología</b>	Disposición física de nodos y medios de red dentro de una estructura de networking empresarial.
<b>Trama</b>	Agrupamiento lógico de información enviado como unidad de capa de enlace de datos a través de un medio de transmisión.

## RESUMEN

En la actualidad Internet ha pasado a formar parte de un medio de comunicación necesario y fundamental en las sociedades, pues se puede observar que hoy en día, en cualquier mercado, ya sea financiero, económico, telecomunicaciones, académico, etc., Internet es una excelente herramienta para cualquier aplicación o tarea que se desee realizar.

Debido a ésta gran importancia de Internet, es de suma importancia que toda su estructura sea robusta y mejorada continuamente. Y una de las partes fundamentales de la estructura de Internet y de las todas las redes de computadoras es el protocolo enrutado IP.

La versión del protocolo enrutado IP que se utiliza actualmente y que se utilizó por mucho tiempo, por su gran poder y escalabilidad, fue el protocolo IPv4, pero desafortunadamente IPv4 quedó pequeño para todo el desarrollo y crecimiento de aplicaciones de las redes de computadoras que actualmente existen. Es por ello que la IETF decidió dar el paso como parte de la evolución misma de IP para llegar a su nueva versión la cual denominaron IPv6 o IPng.

Con IPv6, se aliviará toda la demanda naciente y creciente que se tiene hoy en día de direcciones IP, para cada una de las aplicaciones que se tienen y se tendrán en el futuro. IPv6 ofrecerá poder direccionar  $2^{128}$  nodos, lo que es equivalente a 340,282,366,920,938,463,374,607,431,768,211,456 nodos, debido a que ahora la dirección constará de 128 bits, lo cual elimina muchas de las herramientas que se utilizaban en IPv4 para poder optimizar el espacio de direccionamiento con el que se contaba  $2^{32}$ .

IPv6 trae consigo una ligera modificación en el formato de la cabecera, así como en la forma de direccionar los nodos. Ahora con IPv6, los campos ya no serán campos de 8 bits representados en forma decimal, sino que serán campos de 16 bits representados en forma hexadecimal y que están separados con “:”, lo cual cambia la forma de direccionar, así como elimina o cambia algunas herramientas de enrutamiento y gestión que se venían utilizando con IPv4.

Además IPv6 obliga a los demás protocolos de otras capas a realizar cambios para poder adaptarse a las nuevas funcionalidades que IPv6 trae consigo.

En lo que seguridad trata IETF se aseguró de que IPsec fuera obligatorio para IPv6, con lo cual permite que todas las aplicaciones que se creen sean mucho más seguras de las que se tenían en IPv4. Esta seguridad que agrega IPsec, se agrega únicamente en la capa de Internet, y se puede predecir que en base a las lecciones que se aprendieron con IPv4, en relación a seguridad, IPv6 será más segura que IPv4.

## **OBJETIVOS**

### **General:**

Estar conscientes del estado actual del espacio de direcciones con el que se cuenta en el protocolo IPv4, y poder tener el suficiente conocimiento y las herramientas necesarias para poder realizar la migración, de una manera óptima, al nuevo protocolo enrutado IPv6, y así poder aprovechar de sus bondades y beneficios.

### **Específicos:**

1. Proporcionar una introducción de que son las redes de computadoras, cómo funcionan actualmente, la evolución que pudieron tener, y el papel que desempeñan en nuestras sociedades.
2. Hacer un análisis del funcionamiento y estructura del actual protocolo de enrutamiento IPv4, poder saber cuáles son sus características y así poder determinar cuáles podrían ser sus deficiencias y bondades.
3. Conocer a detalle cuales son las características del nuevo protocolo IPv6, cuáles son los cambios en base al anterior protocolo IPv4 y en base a esto, saber cuáles son los beneficios que trae IPv6.
4. Proporcionar algunas herramientas para poder llevar a cabo, de una manera óptima, la migración a IPv6 en plataformas Windows XP y Cisco.





## INTRODUCCIÓN

Dado al crecimiento rápido de usuarios que desean conectarse a Internet o a redes corporativas que necesitan conectarse con otras redes, el espacio de direccionamiento con el que se cuenta actualmente con el protocolo IPv4, se está acabando. Esto aunado a el rápido desarrollo de nuevas aplicaciones que demandan más direcciones IP, hace darnos cuenta ante la gran problemática de poder contar lo antes posible con un mayor espacio de direccionamiento.

Es por ello que la IETF decidió trabajar en desarrollar un nuevo protocolo, que no es más que una evolución de IPv4, el cual le denominaron IPv6 o IPng. Con éste nuevo protocolo IPv6, el problema de direccionamiento queda resuelto pues ahora se podrán direccionar  $2^{128}$  nodos, lo cual tomando de referencia la población mundial aproximada de 7 mil millones de habitantes, correspondería a cada habitante  $4.8 \cdot 10^{28}$  direcciones IP versión 6, lo cual es suficiente.

En éste trabajo de investigación se realizará una introducción de cómo nacen la redes, cómo han venido evolucionando, así como de un análisis detallado del protocolo actual IPv4. También se analizará todas las características del nuevo protocolo IPv6, y en base a esto y al anterior análisis poder determinar cuáles son los beneficios y bondades de IPv6.

También se darán algunas herramientas, tanto teóricas como prácticas, que serán muy útiles para poder estar listo para cuando se llegue el momento de hacer la migración o crear una nueva red con el protocolo IPv6, dependiendo de cada una de las necesidades.

# **1. INTRODUCCIÓN A LAS REDES**

Desde la creación del primer computador, se pudo observar la gran utilidad de éste en el diario vivir del hombre. Es por ello que el hombre siguió tratando de perfeccionar el computador y hacerlo más compacto, hasta lo que hoy en día cada uno de nosotros tenemos en nuestro hogares o lugares de trabajo.

Actualmente las redes de computadoras desempeñan un papel importante en el desarrollo de las comunicaciones. Esto se puede observar claramente en aquel estudiante que necesita descargar un archivo para terminar su tarea o en el gerente que necesita establecer una videoconferencia con su homólogo en la sede de Chile pues sus limitantes son la distancia y el tiempo.

Se ha podido observar, de acuerdo a los últimos avances, que las telecomunicaciones están estrechamente relacionadas con las redes de computadoras, pues ahora desde muchos teléfonos móviles, se puede acceder a un computador servidor, y de éste poder descargar aplicaciones para el móvil, o poder enviar correos electrónicos que son almacenados en un servidor. Es por ello que en este capítulo haremos un análisis detallado de las redes de computadoras, por desempeñar un papel tan importante hoy en día.

## **1.1 Redes de computadoras**

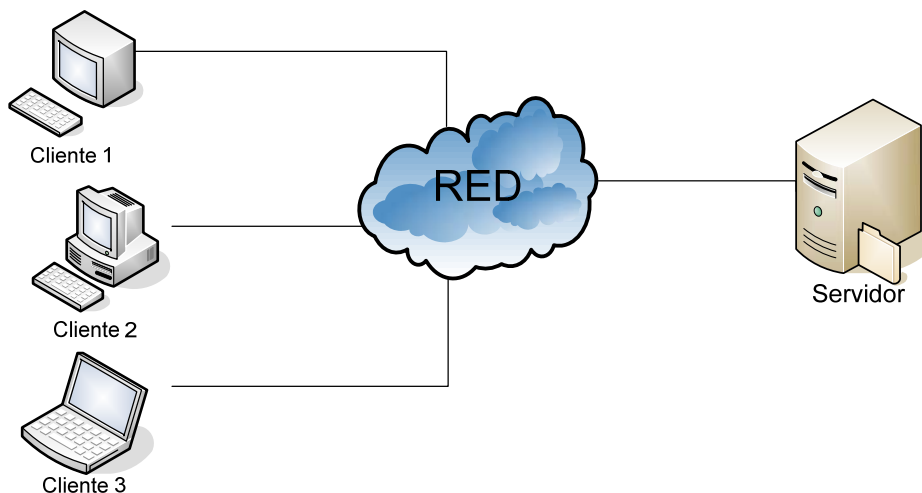
Se define como una red de computadoras al conjunto de computadoras autónomas que están interconectadas, o sea que pueden intercambiar información y compartir recursos, y en la cual la distancia geográfica no es una

limitante. Los medios por los cuales podemos interconectar las computadoras son varios, y el o los factores que se toman en cuenta para elegir entre un tipo u otro podrían ser, factor económico, geográfico, velocidad de transmisión, facilidad de instalación y mantenimiento, etc.

Las redes de computadoras se utilizan en la mayoría de empresas para poder compartir los recursos, que los datos de cada uno de los usuarios estén disponibles para todos los demás usuarios y además para que todos los usuarios se puedan comunicar ya sea por correo electrónico u otro medio.

Los modelos de comunicación entre computadoras que existen en las redes son, el modelo cliente-servidor y el modelo igual-igual. El modelo cliente-servidor es el más utilizado en la redes actuales, pues es aplicable para distancias cortas y para distancias largas. En este modelo existe un servidor, que es una computadora bastante poderosa donde están almacenados todos los datos, y los clientes son las computadoras sencillas que los usuarios tienen en sus oficinas. En la figura 1 se puede observar, este modelo.

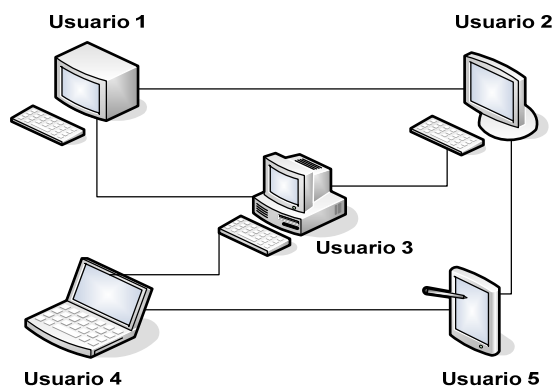
**Figura 1. Modelo cliente-servidor**



Este tipo de redes tienen sus ventajas y desventajas. Una desventaja en una red cliente-servidor es de que existe un único punto de falla, pues si el servidor falla, toda la red falla, otra desventaja son los costos, pues se debe contar con un servidor poderoso así como de un personal capacitado para poder darle soporte al servidor como a los usuarios, por lo tanto los costos aumentan en relación del modelo igual-igual. Con respecto a ventajas, podemos decir que en este tipo de red existe más seguridad, pues cada usuario para poder acceder al servidor debe identificarse, otra ventaja es que todos los datos pueden copiarse de una ubicación central de gran capacidad. Además en este modelo de comunicación se hace más fácil administrar una red de bastantes usuarios.

Como se mencionó anteriormente, el otro modelo es el de comunicación igual-igual. En este modelo cada usuario de un grupo en particular puede comunicarse con una o más personas del grupo, el término cliente y servidor es relativo, pues se considera a cliente a aquella máquina que está haciendo la petición de un archivo y a servidor a aquella que le entrega el archivo a la primera. La figura 2 ilustra este modelo.

**Figura 2. Modelo igual-igual**



En el modelo igual-igual, se conectan las computadoras de los usuarios directamente con las de los demás usuarios. Es utilizado cuando se desea construir redes pequeñas, redes que consten de no más de 10 computadoras, en la cual se desean que cada uno de los usuarios esté compartido con los demás usuarios y así todos puedan transferir y recibir información unos con otros. Este tipo de redes son fáciles y rápidas de construir además de ser económicas, pues lo único que se requiere es que cada máquina tenga el sistema operativo adecuado y el respectivo cableado entre las máquinas. Una desventaja es que no hay mucha seguridad en una red de este tipo pues no hay ningún administrador, además la eficiencia de dicho tipo de red se ve disminuida al aumentar el número de máquinas pues al momento de una máquina actuar como servidor de varios clientes el tiempo de respuesta a cada uno de los clientes se hace más largo, pues una máquina que forma parte de este tipo de redes no se podría comparar con un servidor utilizado en las redes cliente-servidor.

### **1.1.1 Clasificación según distribución de área geográfica**

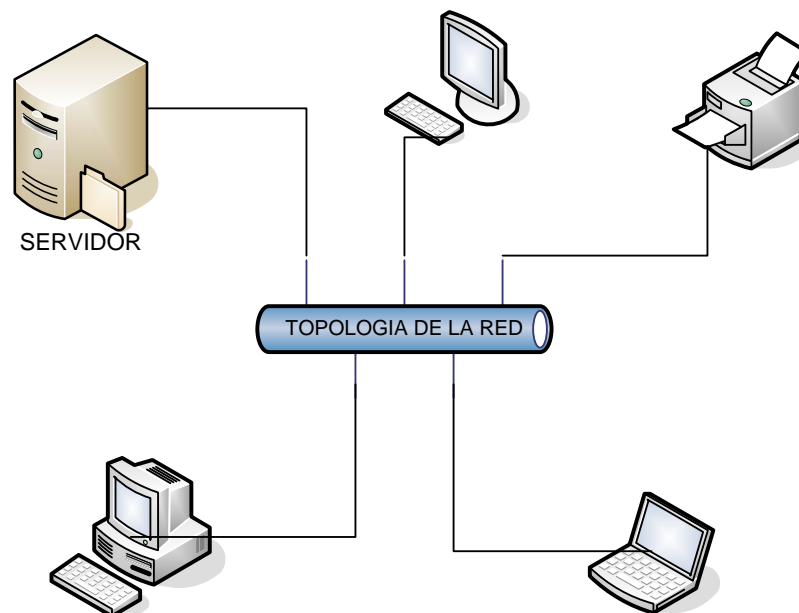
Las redes de computadoras se pueden clasificar según su extensión geográfica, aunque en la realidad estas clasificaciones no son muy fáciles de distinguir. Según su extensión geográfica las redes de computadoras se pueden clasificar en:

#### **1.1.1.1 Red de área local**

A una red de área local también se le conoce como LAN. La palabra LAN se deriva de las siglas en inglés *Local Area Network*, que en español significa red de área local. Este tipo de redes son aquellas de propiedad privada que geográficamente están dentro de un área relativamente pequeña.

Para ejemplificar esto, podríamos considerar una agencia de un centro bancario, esta agencia tiene dentro de sus instalaciones varias computadoras que se conectan a un servidor principal que se encuentra físicamente ubicado en la misma agencia. Cada computadora o host y el servidor interconectados, forman una red a la cual se le denomina por su distribución red de área local. La figura 3 muestra este tipo de red. Las redes de área local tradicionales se ejecutan actualmente a una velocidad de 10 a 100 Mbps ( Mega bits por segundo ), pero según los últimos avances, estas redes podrían llegar a una velocidad medida en giga bits por segundo. Algunas de las topologías lógicas utilizadas en este tipo de redes, pueden ser Ethernet, Token Ring y FDDI, la más utilizada actualmente es Ethernet.

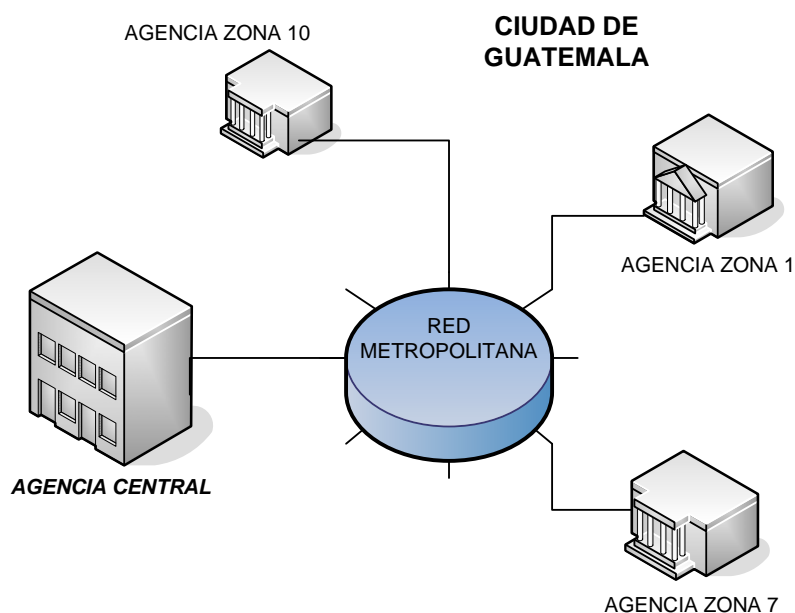
**Figura 3. Ejemplo de red de área local**



### 1.1.1.2 Red de área metropolitana

A este tipo de red también se le conoce como MAN, de sus siglas en inglés, *Metropolitan Area Network*, que traducidas a español significan red de área metropolitana. Una MAN consta generalmente de dos o más LAN dentro de un área geográfica común. Una MAN puede abarcar un área geográfica equivalente a una ciudad, o aproximadamente 10 kilómetros entre procesadores. Continuando con el ejemplo de las agencias bancarias, se puede considerar a una MAN como la red que se forma cuando interconectamos a todas las agencias dentro de la ciudad y todas teniendo comunicación con la agencia central. Este ejemplo de una red MAN se ilustra en la figura 4.

**Figura 4. Ejemplo de red de área metropolitana**





En la figura 4 se pudo observar edificios comunicados unos con otros por medio de la red metropolitana. El tipo de enlace que existe entre cada agencia es un enlace que se realiza por medio de las interfases seriales de un enrutador. Cada LAN ubicada dentro de los edificios en la figura 4, puede comunicarse con las LAN de los demás edificios por medio de enrutadores (routers), que son los encargados de enrutar todo el tráfico cursado.

### **1.1.1.3 Red de área extensa**

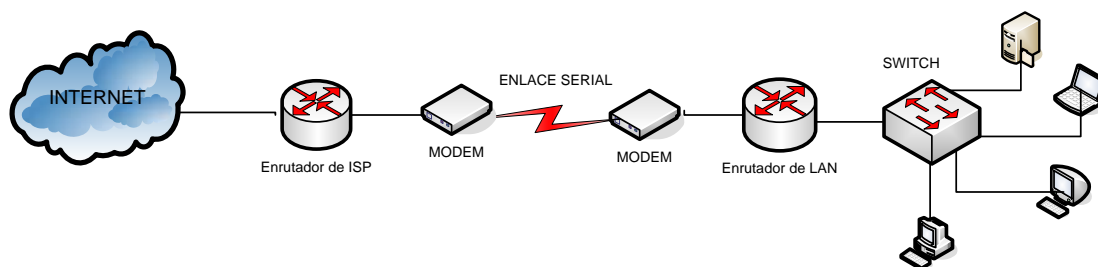
A este tipo de red también se le conoce como WAN, por sus siglas en inglés, *Wide Area Network*, que traducidas significan red de área amplia o extensa. Las redes de área amplia se utilizan para interconectar las redes LAN que anteriormente mencionamos. Se les denomina redes de área amplia, pues las longitudes que recorren los cableados entre un dispositivo y otro son más de un kilómetro, a diferencia de una red de área local que el cableado tiene como longitud máxima 1000 metros entre procesadores. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes. Una WAN está diseñada para operar entre área geográfica extensas, ofrecer recursos remotos de tiempo completo y en tiempo real, conectado a servicios locales. Algunas tecnologías utilizadas en las redes de área amplia son:

- Red digital de servicios integrados (RDSI o sus siglas en inglés ISDN)
- Línea de suscripción digital ( siglas en inglés DSL )
- Retransmisión de trama o Frame relay.
- Red óptica síncrona (siglas en inglés SONET ).

Frecuentemente, las WAN utilizan instalaciones de transmisión provistas por los proveedores de servicios de telecomunicaciones, como por ejemplo Telefónica, Newcom, Navega y Telgua.

Una red de área amplia o extendida es la que se forma por un enrutador, al cual están conectados todos los hosts de una LAN, y el enrutador del proveedor de servicio de Internet o ISP (*Internet Service Provider*). El tipo de enlace que existe entre el enrutador del cliente y el enrutador del ISP utiliza una interface serial, a diferencia de una LAN que utiliza una interface ethernet o fastethernet, dependiendo de la configuración de la velocidad de ésta. Una WAN se ilustra en la figura 5.

**Figura 5. Ejemplo de red de área extensa conexión a internet**



En la figura 5 se observa una WAN en la cual se conecta por medio de un enlace serial, toda una LAN hacia la nube de Internet. No necesariamente tiene que conectarse a Internet, sino que también se podría utilizar una WAN para interconectar dos LAN remotas que estén separadas por una gran distancia.

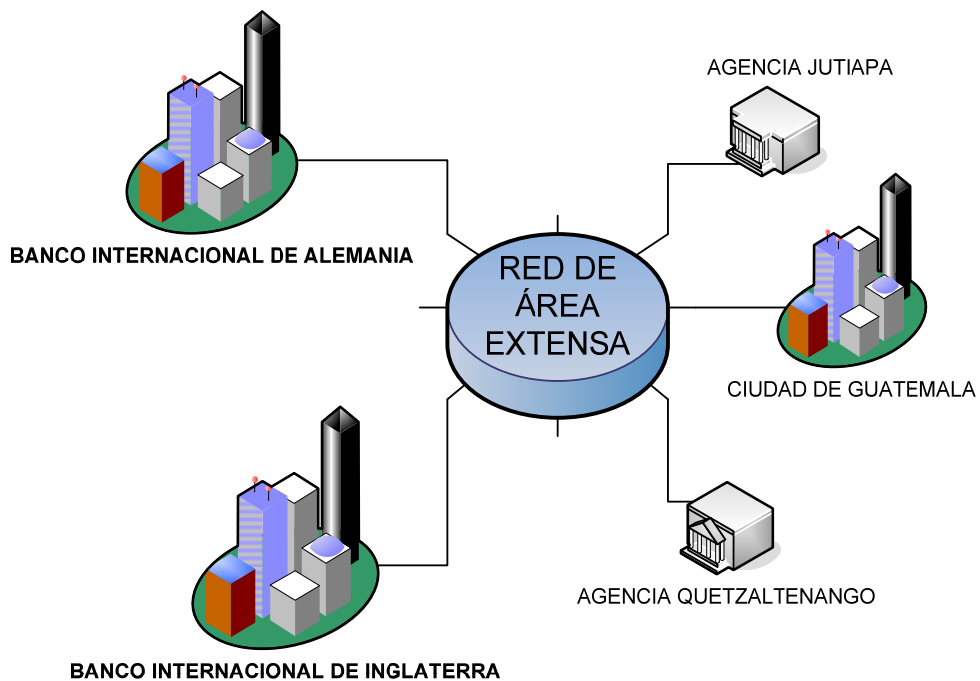
En los enlaces WAN se habla del tipo de encapsulamiento para establecer la comunicación. Los tipos de encapsulamientos pueden ser:

- PPP ( *Point to point protocol* o protocolo de punto a punto)

- HDLC ( Control de enlace de datos de alto nivel )

Una WAN puede abarcar un país, un continente e incluso un planeta. Esto quiere decir que se puede considerar Internet como una red WAN, pues ésta abarca todo el planeta. Tomando nuevamente el ejemplo de las agencias bancarias, se puede decir que una WAN es la que se construye cuando unimos por medio de enlaces las agencias de todo el país de Guatemala, y establecemos enlaces con otras agencias en el interior de Guatemala y con bancos de otros países. Esto se puede observar en la figura 6.

**Figura 6. Ejemplo de WAN agencias bancarias**



En una WAN, a diferencia de una LAN que utiliza dispositivos como las tarjetas de interfaz de red (NIC) y los switch, los dispositivos utilizados son los siguientes:

- Los enrutadores ( routers )
- Los modems (modulador / demodulador). En este dispositivo se consideran dos tipos. El primero de ellos son las unidades de servicio de canal / unidades de servicio de datos ( CSU/ DSU ) que realizan la interfaz con los servicios T1/ E1, y el segundo tipo son los adaptadores de terminal / terminación de red 1 ( TA / NT1 ) que realizan la interfaz con los servicios de red digital de servicios integrados (RDSI).

Los enrutadores se pueden utilizar en una LAN, pero su uso es diferente, pues en este tipo de red se utiliza para aumentar los dominios de broadcast o sea para segmentar una red y con ello obtener subredes. En una WAN sus funciones principales son, elegir la mejor ruta para enviar los paquetes y la de conmutación de los paquetes a la interfaz correcta.

Todos los estándares WAN son definidos por varias autoridades dentro de las cuales podemos mencionar las siguientes:

- Fuerza de Tareas de Ingeniería de Internet ( IETF )
- Organización Internacional de Normalización ( ISO )
- Sector de Normalización de Telecomunicaciones de la Unión Internacional de Telecomunicaciones ( UIT-T )
- Asociación de Industrias Electrónicas ( EIA )

#### 1.1.1.4 Red de área de almacenamiento

A este tipo de red también se le denomina SAN, por sus siglas en inglés *Storage Area Network*, que traducidas al español significan red de área de almacenamiento. Este tipo de red, es una red dedicada para trasladar datos entre servidores y recursos de almacenamiento, es una red de alto rendimiento. Como es una red separada y totalmente dedicada al almacenamiento, se evita de conflicto con el tráfico de cliente y tráfico de servidores. Este tipo de red surgió de las necesidades de las empresas de tener un área de almacenamiento de información de cada uno de los servidores, pues por ejemplo si tenemos una empresa transnacional que está integrada por más de 3000 trabajadores, y cada uno de los trabajadores maneja una cuenta de correo electrónico, el o los servidores de correo electrónico de dicha empresa debe de tener un área de almacenamiento, posiblemente remoto, donde deben de almacenar toda la información correspondiente con dichos correos. Es por ello que se crea un enlace dedicado solamente para la comunicación entre los servidores y el área de almacenamiento.

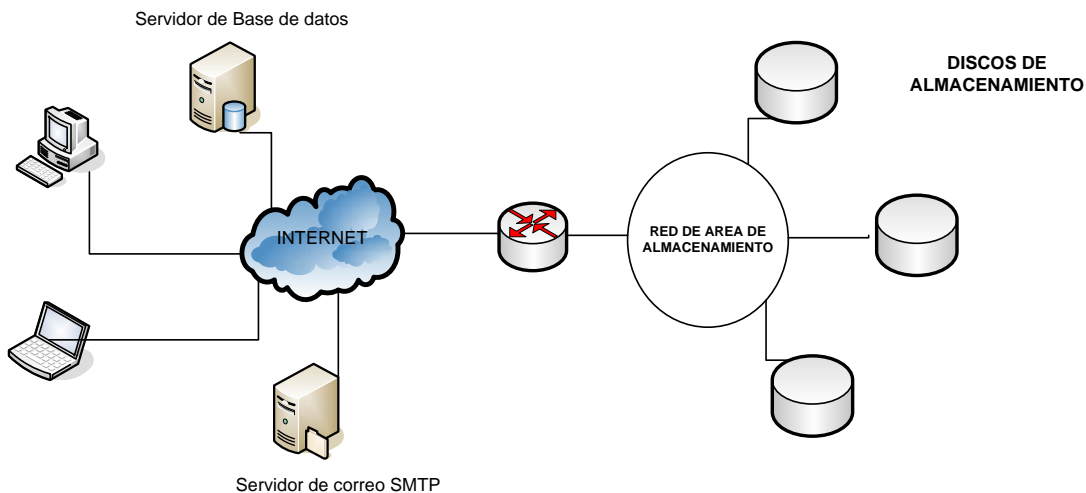
Una SAN debe de poseer algunas características como dentro de las cuales podemos mencionar:

- Rendimiento, las redes de almacenamiento permiten el acceso a recursos de almacenamiento como lo son las matrices de disco o de cinta, por parte de dos o más servidores simultáneamente.
- Disponibilidad, este tipo de red tiene una tolerancia a los desastres, ya que se puede hacer una copia exacta de los datos mediante una SAN, hasta una distancia de diez kilómetros.
- Escalabilidad, cuando nos referimos a escalabilidad, nos referimos a que puede usar una amplia variedad de tecnologías, ya sea más rápida o

más lenta. Esto permite la fácil reubicación de datos de copia de copias de seguridad y de todos los archivos que almacenamos.

Este tipo de red se puede observar en la figura 7.

**Figura 7. Ejemplo de red de área de almacenamiento**



### 1.1.2 Topología de red

Una topología define la estructura de una red. Cuando se habla de la topología física se habla de la distribución real de los cables y como quedan distribuidos los distintos dispositivos de redes, entiéndase por dispositivos de redes a los conmutadores, enrutadores, hubs, repetidores, etc. La otra parte es la topología lógica, que define la forma en que los hosts o computadoras acceden a los medios para enviar los datos.

### **1.1.2.1 Topologías físicas de LAN**

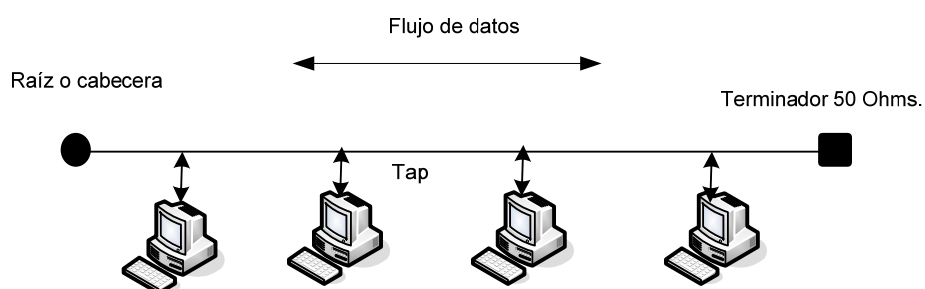
Las topologías físicas de LAN se refieren a la forma en que están distribuidos los cables y los dispositivos de red. Las topologías usuales en LAN son bus, árbol, anillo, estrella y estrella extendida.

#### **1.1.2.1.1 Topología en bus y árbol**

En una red con topología en bus todos los hosts o estaciones se encuentran conectadas directamente, a través de interfaces físicas conocidas como tomas de conexión, a un medio lineal o bus. Una transmisión desde cualquier estación se propaga a través de todo el medio en ambos sentidos y es recibida por las demás estaciones. El tipo de comunicación que existe entre el host y la toma de conexión es full-duplex, esto permite la transmisión de datos a través del bus y la recepción de datos desde éste. En este tipo de red existe un terminador de 50 ohmios que absorbe las señales, eliminándolas del bus. En esta topología se utiliza cable coaxial y las tomas o taps eran tomas en forma de "T". Una de las desventajas de este tipo de red, es que para comunicarse con un host en específico la información debe de pasar por todos los demás hosts, lo que genera más tráfico y esto puede elevar el nivel de colisiones en el medio. Algunas tecnologías de topologías de bus son, 10BASE-2 y 10BASE-5 en ethernet, o también denominadas thinnet y thicknet respectivamente, éstas se detallaran más adelante. La topología en bus se puede observar en la figura 8. Una red construida con topología en bus, es el tipo de red más fácil de conectar, porque su estructura es un canal único por donde fluyen los datos en una señal de 50 ohmios utilizando un cable coaxial RG58, con terminadores (resistencias) de 50 ohmios en los extremos y "T" que miden 25 ohmios para la entrada en las computadoras. Algunas de las características de esta

topología son, velocidad de 10 Mbps como máximo, es más barato, más inestable y necesita más mantenimiento.

**Figura 8. Ejemplo de topología física en bus**



Un detalle importante a considerar está relacionado con el equilibrado de las señales, pues la potencia del emisor debe estar comprendida entre límites, donde no sea muy baja para que la señal se pierda en el recorrido del medio ni donde sea demasiada alta para distorsionar la señal transmitida. Si una estación desea transmitir hacia otra, el equilibrado de la señal se debe realizar para todas las permutaciones de estaciones tomadas de dos en dos, esto quiere decir que para  $n$  estaciones, el número de permutaciones es  $n * (n-1)$ .

Los medios de transmisión utilizados para esta topología de red son, el par trenzado, el cable coaxial de banda base, el cable coaxial de banda ancha y la fibra óptica. De estos medios de transmisión el más utilizado en la topología de bus o árbol fue el cable coaxial de banda base. Los detalles de cada uno de los medios de transmisión anteriormente descritos se detallarán más adelante.

Con respecto a la topología en árbol, se puede decir que es una generalización de la topología en bus, pues ésta tiene más ramificaciones. Se



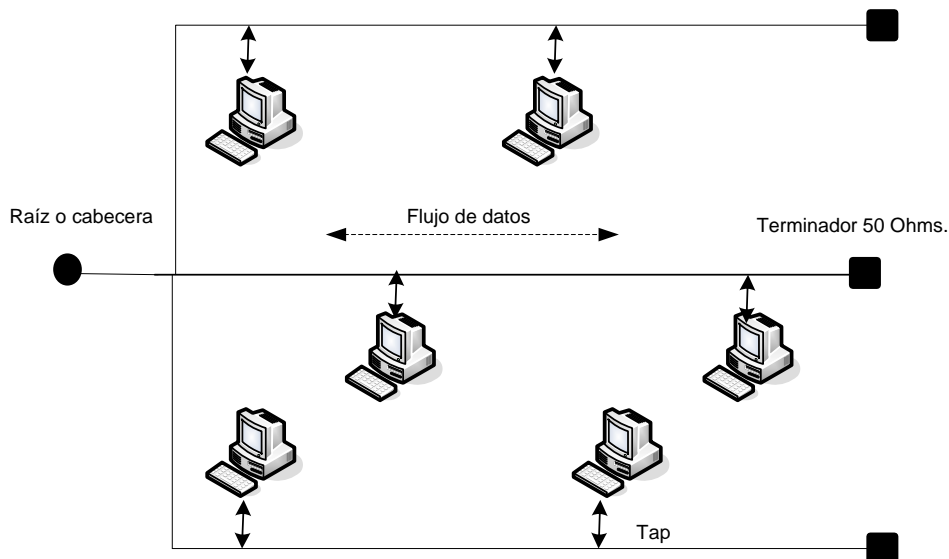
podría decir que una topología en bus es una topología en árbol, pero con una sola rama. El medio de transmisión es un cable ramificado sin caminos cerrados, pues al igual que la topología en bus, éste también utiliza terminaciones. Las ramificaciones comienzan en un punto conocido como raíz o cabecera (*headend* en inglés ). Cada una de estas ramas puede tener a su vez más ramificaciones.

La forma de transmisión de la topología árbol es igual a la topología en bus. Si alguna estación transmite, todas las demás estaciones reciben el mensaje y verifican si es para ellos el mensaje, si el mensaje no es para ellos, lo dejan pasar a la siguiente estación y así sucesivamente hasta que el mensaje llega a la estación destino donde es copiada por la estación pero de igual forma deja pasar el mensaje hasta que se atenúa en el terminador de 50 ohmios. Esto se logra por medio de que el mensaje a transmitir se transmite en bloques pequeños denominados tramas, en las tramas van incluidos los datos propiamente del mensaje, también denominados paquetes, y además también se incluye información de control, sincronización y de identificación, para que el mensaje sea reconocido y tomado por la estación destino requerida. Tanto la topología en bus como la de árbol, se caracterizan por el uso de un medio multipunto. Este tipo de topología se utilizaba mucho en los principios de los años 1990, pero se observó que esta topología era muy vulnerable a las desconexiones, pues si una estación que formaba parte del bus se desconectaba por alguna razón, toda la comunicación se perdía de ahí en adelante. Este tipo de desconexión era muy fácil de que ocurriera, pues el cableado tenía que llegar a la altura de la NIC (*Network Interface Card* o tarjeta de red) y si alguien pasaba cerca del CPU (*Central Process Unit* o unidad central de proceso), que es donde se conecta el cable coaxial por medio de la NIC, fácilmente se desconectaba el cable coaxial del tap en forma de "T". Es

por ello en la actualidad esta topología física de red ya no se utiliza muy frecuentemente. La figura 9 ilustra una topología en árbol, con tres ramas.

En una red utilizando topología árbol o bus, a diferencia de la topología en anillo, es de que el bus o árbol es pasivo, o sea que no se produce regeneración de las señales en cada nodo, no necesita de repetidores para regenerar la señal y que no se atenúe en el transcurso del recorrido, como se hace en una topología en anillo.

**Figura 9. Ejemplo de topología física en árbol**

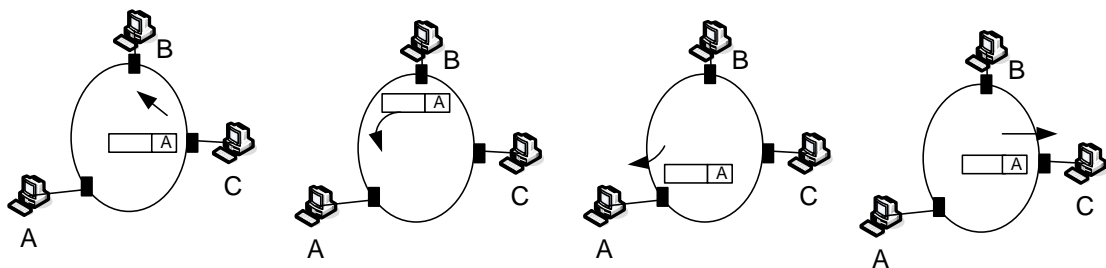


#### 1.1.2.1.2 Topología en anillo

En esta topología, la red consta de un conjunto de repetidores unidos por enlaces punto a punto formando un circuito cerrado. El repetidor es un dispositivo que trabaja en la capa 1 del modelo referencia OSI, que es capaz de

recibir los datos representados por bits, amplificarlos y retransmitirlos para que pueda alcanzar una longitud mayor en el medio, y no se atenúen por éste. Los enlaces son unidireccionales, es decir, los datos se transmiten sólo en un sentido, de modo que éstos circulan alrededor del anillo en el sentido de las agujas del reloj o en el contrario. Cada estación se conecta a la red mediante un repetidor, transmitiendo los datos hacia la red a través de él. Al igual que en las anteriores topologías, la información se transmite en tramas, las cuales circulan por todo el anillo y pasan por todas las estaciones, y cuando llegan a la estación destino, ésta copia la trama la cual sigue por todo el anillo hasta llegar nuevamente a la estación que la originó, donde es eliminada. En la figura 10 se representa el proceso del envío de una trama del host C al host A.

**Figura 10. Ejemplo de topología física en anillo.**



Para que un anillo funcione como una red de comunicaciones son necesarias tres funciones: inserción de datos, recepción de datos y eliminación de datos, las cuales son llevadas a cabo por los repetidores. Cada repetidor, además de servir como un elemento activo en el anillo, sirve como punto de conexión de dispositivo. Los repetidores realizan las funciones de inserción y recepción de datos de forma diferente a las tomas "T" que sirven como puntos de conexión de dispositivos en un bus o en un árbol. La eliminación de datos es, sin embargo, más complicada en el caso de un anillo. Las señales en un bus se insertan en una línea, se propagan hacia los extremos y son absorbidas

por los terminadores. En un anillo los paquetes pueden ser eliminados ya sea por la estación destino o por la estación origen, pero ésta última opción es mejor debido a que permite confirmaciones o acuses de recibo y permite además direccionamiento múltiple pues el paquete es enviado a múltiples estaciones. Las formas o estrategias de cómo ingresar el paquete al medio se les denomina protocolos de control de acceso al medio. En la topología en anillo, los métodos de acceso que se utilizan para poder acceder al medio son el Token Ring y el FDDI, en los cuales la estación que transmite es la que posee el token o estafeta mientras los demás reciben, este método de acceso se detallará más adelante.

El repetidor puede tener dos objetivos, el primero es contribuir al funcionamiento adecuado del anillo dejando pasar todos los datos que lo atraviesan y el segundo es de ofrecer un punto de acceso a las estaciones conectadas para transmitir y recibir datos. Cuando el repetidor está recibiendo datos se dice que está en estado de escucha, en este estado cada bit recibido se retransmite con un retardo que aproximadamente es igual al orden de la duración de un bit. En el estado de transmisión el repetidor transmite el repetidor recibe bits de la estación y los retransmite por la línea de salida. Existe un tercer estado que es el estado de cortocircuito en el cual el repetidor está cortocircuitado por un relé, de manera que las señales propagadas atraviesan el repetidor sin más retardo que el de propagación en el medio. En enlaces repetidor a repetidor es posible utilizar varios medios físicos de comunicación, entre los cuales están el par trenzado, el cable coaxial de banda base y la fibra óptica.

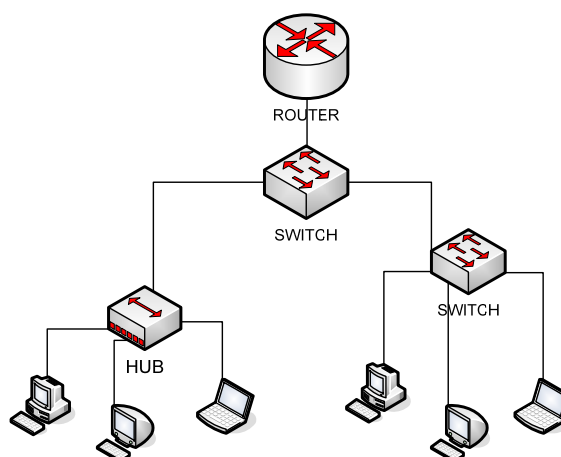
La topología en anillo presenta problemas que deben de ser considerados en un diseño de red, como por ejemplo la rotura de un enlace o el fallo en un repetidor hace que toda la red deje de funcionar, la instalación de un nuevo

repetidor para poder conectar nuevos dispositivos a la red necesita la identificación de los repetidores adyacentes, y el tráfico innecesario cursado dentro de el anillo debido a que el paquete debe de cursar todo el anillo hasta regresar a la estación origen y que así sea eliminada.

### 1.1.2.1.3 Topología en estrella

En una red con esta topología cada estación está directamente conectada a un nodo central, generalmente a través de dos enlaces punto a punto, una para transmisión y otro para recepción. Además se destacan los niveles jerárquicos, pues cada uno de los dispositivos que se utilizan en ésta topología pertenece a uno de estos niveles. Se puede decir que una estrella está formada primeramente en el nivel más bajo por cada una de las estaciones que se van a interconectar, en el segundo nivel están los hubs o concentradores, en el tercer nivel están los switches y en el último nivel se encuentran los enrutadores. La figura 11 muestra este esquema para una mejor comprensión:

**Figura 11. Ejemplo de topología en estrella.**



Cada uno de estos dispositivos pertenece a un nivel jerárquico distinto debido a que operan en una capa diferente del modelo de referencia OSI, esto se verá más adelante a detalle.

En esta topología aunque la disposición física sea la de una estrella, lógicamente funciona como un bus, esto es debido a la forma en que la topología lógica utilizada accede al medio y como es transmitido la trama de ella.

Esta topología es la más utilizada en la actualidad, pues es una topología fácil de diseñar, rápida y barata de implementar y es muy escalable. Cuando nos referimos a escalable, nos referimos a que la red la podemos hacer crecer muy fácilmente, con sólo agregar un dispositivo más y agregar unos cableados, podemos extender la red. Además cuando decimos escalable también nos referimos a que podemos optar por una tecnología más reciente que transmita a mayores velocidades sin hacer cambios tan drásticos en lo que ya se tiene cableado.

#### **1.1.2.2 Topologías lógicas**

Cuando hablamos de las topologías lógicas de red, nos referimos al método o la forma en que cada una de las tramas enviadas por las estaciones puede acceder al medio físico para que éstas sean conducidas a su destino. El método de acceso más utilizado en la actualidad es CSMA/CD que es el que utiliza Ethernet. El segundo método utilizado es el de paso de testigo o "token" que es el que utilizan token ring y FDDI. Cada una de estas topologías lógicas se detalla a continuación.

### **1.1.2.2.1 No determinísticas**

La topología no determinística se refiere a una red que utiliza protocolos donde la trama que se envía de un host o estación "A" a una estación "B" debe de escuchar el medio y poder determinar si es capaz de transmitir en ese momento. Esto quiere decir que en esta topología la estación emisora debe de corroborar que el medio físico por el cual desea transmitir está disponible para poder transmitir, de estar disponible se transmite la trama de no ser así la estación origen debe de esperar hasta que el medio esté libre y en ese momento puede transmitir. Dicho en otras palabras se podría decir que el primero que llegue es el primero que sirve. El protocolo que se utiliza en estas redes con topología no determinística es Ethernet.

#### **1.1.2.2.1.1 Ethernet**

Ethernet se basa en el trabajo de Robert Metcalf, David Bogas y otros científicos que trabajaron conjuntamente en el Centro de Investigación de Palo Alto de Xerox en los finales de los años de 1970. La primera red se denominó Ethernet en honor al éter, la sustancia mítica que permitía el viaje de la luz a través del espacio. La primera norma Ethernet, DIX 1.0 se creó en 1980, y se le denominó DIX en honor a las empresas que participaron en su creación que fueron, *Digital Equipment Corporation*, Intel y Xerox. A esta versión la IEEE le denominó Ethernet IEEE 802.3.

Todas las LAN y MAN constan de un conjunto de dispositivos que deben compartir la capacidad de transmisión de red, de manera que se requiere algún método de control de acceso al medio con objeto de hacer un uso eficiente de esta capacidad. Esta es la función del protocolo de control de acceso al medio MAC (*Media Access Control*), que está situada en la capa 2 del modelo de

referencia OSI. Los métodos de control de acceso son sistemas que permiten que muchos nodos puedan acceder a un medio de red compartido mediante la concesión organizada de accesos. Ethernet utiliza un método de control de acceso denominado detección de portadora, su nombre completo es Acceso Múltiple por Detección de Portadora o CSMA/CD (*Carrier Sense Multiple Acces / Collision Detect*). Este método CSMA comúnmente se le denomina “escuchar antes de hablar”, pues cada una de las estaciones primero escucha el medio, para poder detectar si hay alguna otra estación que está transmitiendo, y si el medio está libre entonces la estación transmite. La parte de detección de colisiones es porque este método puede detectar las colisiones. Entiéndase por colisiones, al evento cuando dos paquetes se chocan por ser transmitidos simultáneamente en el mismo medio. Los nodos Ethernet detectan las colisiones manteniéndose a la escucha mientras transmite, si se produce una colisión, los nodos miden que el voltaje que recibieron de la última muestra que tomaron del medio es una señal del doble de voltaje que el esperado. Una vez detectada la colisión las NIC de cada una de las estaciones envían una señal de atasco o Jam que indica a todos los nodos de la red que no es un buen momento de enviar paquetes pues ha habido una colisión, entonces cada una de las estaciones esperan un tiempo variable para poder volver a transmitir, este tiempo variable es determinado por un algoritmo de postergación propio de cada dispositivo de la red.

Ethernet es una familia de tecnologías para redes que incluye Legacy, Fastethernet y Gigabitethernet. Las velocidades de ethernet pueden ser 10, 100, 1000, ó 10000 Mbps (Mega bits por segundo).

La operación de ethernet abarca las primeras dos capas del modelo de referencia OSI, la capa física y la primera mitad de la capa MAC denominada LLC o Control de Enlace Lógico (*Link Layer Control*). La movilización de los



datos entre una estación ethernet y otra se hace a través de repetidores, todas las demás estaciones del mismo dominio de colisión ven el tráfico que pasa a través del repetidor. El dominio de colisión es el segmento de red física donde pueden ocurrir errores. Los tipos de dispositivos que interconectan los medios definen los dominios de colisión. Los dispositivos de capa 2 y 3 del modelo OSI dividen o segmentan el dominio de colisión.

El repetidor es responsable de enviar todo el tráfico al resto de puertos, y a la vez es responsable de regenerar o amplificar la señal si ésta fuera distorsionada o atenuada en su transcurso por recorrido del medio físico.

Ethernet cuenta con un sistema de identificación para poder identificar cada una de las interfaces de manera exclusiva. Ethernet utiliza una dirección MAC que consta de 48 bits de largo y se expresan en 12 dígitos hexadecimales. Los primeros 6 dígitos hexadecimales identifican al fabricante del dispositivo, esta porción se conoce como Identificador exclusivo organizacional, y los siguientes 6 dígitos representan el número de serie del dispositivo que lo identifican de forma única. Las direcciones MAC se graban en la memoria ROM (*Read Only Memory*) o memoria de sólo lectura del dispositivo y se copian a la RAM (*Random Access Memory*) o memoria de acceso aleatoria de la estación cuando se inicializa el dispositivo. La NIC utiliza la dirección MAC para evaluar si el mensaje se debe pasar o no a las siguientes capas del modelo OSI.

En ethernet cuando un dispositivo envía datos hacia otro dispositivo, el dispositivo origen adjunta un encabezado con la dirección MAC destino y envía los datos a la red, en el transcurso cada NIC verifica, comparando su dirección MAC con la especificada en la trama, si la trama no le corresponde y si no hay concordancia ésta descarta la trama, cuando la trama llega a su destino, la NIC hace una copia y pasa la trama hacia las siguientes capas superiores. Con lo

anterior se entender que cada estación o nodo ethernet debe de verificar la trama.

La comunicación entre dispositivos se logra por medio del entramado, ésta se efectúa en la capa 2 del modelo OSI. En esta trama viaja información esencial que hace realidad la comunicación, alguna de la información que viaja en la trama es, las direcciones MAC de los dispositivos que se están comunicando, cuándo comienza y cuándo termina la comunicación, método de detección de errores y quién está habilitado para transmitir. Una trama es la unidad de datos de la capa 2 de OSI. Dependiendo de la velocidad a la que transmite ethernet, así va a variar la trama, a nivel de capa física pues en la capa de enlace casi todas las tramas se parecen, pero una trama genérica se podría considerar que está formada por los siguientes campos:

- campo de inicio de trama
- campo de dirección
- campos de longitud y tipo
- campos de datos
- campos de secuencia y verificación de errores

En la figura 12 se ilustra la trama genérica de ethernet.

**Figura 12. Estructura de la trama genérica Ethernet.**

Inicio de trama	Dirección	Longitud y tipo	Datos	Secuencia y verificación de errores
-----------------	-----------	-----------------	-------	-------------------------------------

Entrando un poco más en detalle, los campos de Ethernet IEEE 802.3 son el preámbulo, el delimitador de inicio de trama (SFD), la dirección MAC destino,

la dirección MAC origen, campo de longitud y tipo, el campo de datos con su relleno y el campo de secuencia de verificación de trama (FCS). Este tipo de trama se ilustra en la figura 13 donde además se indica el tamaño de cada trama en bytes.

**Figura 13. Estructura de la trama IEEE 802.3**

Preámbulo (7)	SFD (1)	Dirección destino (6)	Dirección origen (6)	Longitud/ Tipo (2)	Datos Relleno (46 a 1500)	FCS (4)
------------------	------------	--------------------------	-------------------------	--------------------------	------------------------------	------------

(#) = Longitud del campo en bytes

El campo preámbulo es un patrón alternado de unos y ceros (10101010) que se utiliza para la sincronización entre la estación origen y la destino. Este campo se utiliza sólo en versiones de ethernet de 10 Mbps y menores pues en las mayores a esta velocidad se sigue utilizando aunque sea redundante, pero se hace con el objetivo de compatibilidad, por ejemplo en una Fastethernet que transmite a full-duplex a 100 Mbps ya no es necesario el preámbulo pero se utiliza por compatibilidad con las anteriores. El campo SFD (*Start frame delimitator*) o delimitador de inicio de trama es una octeto que marca el final de la sincronización y contiene la secuencia 10101011. El campo de dirección destino, contiene la dirección MAC del dispositivo destino, el mismo concepto se utiliza para el campo de dirección origen. El campo longitud/tipo admite dos posibles usos. Si el valor es menor a 1536 entonces el valor indica la longitud. La interpretación de la longitud se utiliza cuando la capa LLC proporciona la identificación del protocolo, la longitud indica la cantidad de bytes de datos que sigue este campo. El valor tipo especifica el protocolo de la capa superior que va a recibir los datos. Los campos datos y relleno puede tener longitud variable siempre y cuando no excedan la MTU, según la versión de ethernet. La MTU

es la unidad máxima de transferencia permitida (*Maximum Transfer Unit*). Si los datos que se están enviando no completan la MTU se insertan unos rellenos para que la trama cumpla con la longitud mínima admisible, esto variará según la versión de ethernet, para ethernet IEEE 802.3 es 64 bytes. El campo de chequeo de secuencia de trama (FCS) contiene un chequeo de redundancia cíclica (CRC) de 4 bytes, creado por el emisor y recalculado por el receptor que se utiliza para la verificación de tramas erradas. Si hubo errores en la transmisión de la trama, el emisor no puede detectar eso, es por ello que se debe iniciar la retransmisión de la trama por un protocolo de capa superior que sea orientado a conexión que provea el control de flujo de datos.

El método CSMA/CD realiza tres funciones, la primera es de transmitir y recibir paquetes de datos, la segunda es decodificar paquetes y verificar que las direcciones sean correctas antes de transferirlos a las capas superiores del modelo OSI y la tercera es la detectar errores dentro de los paquetes de datos o en la red. Como se mencionó ethernet es una topología con presencia de colisiones. Una típica colisión se puede dar cuando una estación está transmitiendo, pero debido a que la señal eléctrica tarda un tiempo en transportarse por el medio físico que es lo que se le denomina retardo, y esta señal entra a un repetidor el cual le introduce una pequeña latencia en el envío de la trama al puerto siguiente, entonces como suma de estos tiempos es posible que otra estación haya escuchado el medio y como ya no están transmitiendo, ésta comience a transmitir, pero la trama de la última estación que transmitió aún está en el medio, entonces se produce una colisión. Esto sucede en una transmisión half-duplex pues en una full-duplex no sucede.

En las tramas ethernet debe de existir un espacio mínimo al cual se le denomina espacio entre tramas. Este se mide desde el último bit del campo FCS de la última trama hasta el primer bit del preámbulo de la segunda trama.

En ethernet de 10 Mbps, una vez enviada una trama se debe esperar 96 tiempos de bit y cada tiempo de bit es de 100 nano segundos (ns), antes de que se pueda volver a enviar otra trama. En las versiones más veloces de ethernet el tiempo sigue siendo 96 tiempos de bit, pero en cada una de éstas el tiempo de bit es menor. Esto se detallará más adelante.

Como se mencionó, ethernet es una tecnología donde existen colisiones a diferencia de FDDI y Token ring donde no existen colisiones. Las colisiones representan pérdida de ancho de banda que equivale a la suma de la transmisión inicial y a la señal de congestión de la colisión. Existen tres tipos de colisiones que son, las colisiones locales, las colisiones remotas y las colisiones tardías. Las colisiones locales, son las producidas por choques de tramas que provienen de estaciones de un mismo segmento físico de la red, este choque de las tramas produce un aumento en el nivel de voltaje que distorsiona la señal y se detecta como colisión. Con las colisiones remotas, lo que sucede es que las tramas no presentan duplicación de voltaje, pues este tipo de colisiones se da en los extremos más lejanos de una conexión con repetidores, el repetidor no puede enviar el exceso de voltaje, este tipo de colisión es el que más se observa con cable UTP. Las colisiones tardías son las que suceden después de haber enviado los primeros 64 bytes de datos (estos 64 bytes están conformados por la suma de los 7 bytes de preámbulo, 1 byte de FCS, 12 bytes de direcciones MAC, 2 bytes de longitud/tipo y los primeros 42 bytes de datos). La diferencia entre una colisión tardía y las colisiones que se producen antes de los primeros 64 bytes, es que la NIC retransmite de forma automática una trama que ha sufrido una colisión normal, lo cual no sucederá con la tardía.

En ethernet la longitud mínima de la trama es de 64 bytes, y esto es debido a que se desea asegurar que no ocurran colisiones, pues con esto ethernet es capaz de distinguir una trama real de la basura. Estos 64 bytes son

el resultado de haber sumado los campos de dirección destino, dirección origen, tipo y relleno ( $6+6+2+46= 64$ ). El hecho que sean 64 bytes además se puede explicar con lo siguiente, para una LAN de 10 Mbps con una longitud máxima de 2500 metros y cuatro repetidores, el tiempo de ida y vuelta incluyendo la latencia de cada uno de los repetidores se ha determinado a aproximadamente  $50 \mu\text{s}$  (microsegundos) en el peor caso. A 10 Mbps, un bit tarda  $1/10,000,000$  ó sea 100 nanosegundos, con lo cual se puede determinar entonces que 500 bits se tardarán  $50 \mu\text{seg}$ , los 500 bits se redondean a 512 bits (por margen de seguridad) y esto en bytes son 64 bytes. Si la porción de datos de una trama es menor que 46 bytes, el campo de relleno se utiliza para rellenar la trama al tamaño mínimo. Otra razón para tener una trama de longitud mínima es evitar que una estación complete la transmisión de una trama corta antes que el primer bit de ésta misma trama llegue al extremo más alejado del cable, lo cual podría causar una colisión con otra trama enviada por otra estación quien al ver que ninguna otra estación estaba transmitiendo, comenzó a transmitir.

Ejemplificando lo descrito en el anterior párrafo, cuando una estación A envía una trama en el tiempo 0 en un extremo de la red, esta trama tarda un tiempo  $\tau$  en llegar al otro extremo de la red, pero como la trama es muy pequeña y ya A ha terminado de enviar la trama (en el tiempo  $\tau-\epsilon$ ), entonces la estación más distante B comienza a transmitir justo en ese momento, pero como la trama de A todavía no ha llegado a su destino, se produce una colisión y B detecta un aumento en la potencia de la señal, con lo cual sabe que ha ocurrido una colisión y procede a cancelar la transmisión de la trama, momentos después de cancelar la transmisión, B envía 48 bits para avisar a las demás estaciones que hubo una colisión, la estación A escucha este aviso en el momento  $2\tau$ , tiempo en el cual su transmisión ya ha terminado y por consiguiente para A como que no hubiera habido ninguna colisión y no se

preocupa por volver a enviar la trama. Cada estación espera un tiempo aleatorio después de haber escuchado la ráfaga de ruido que envió B.

Luego de haber ocurrido una colisión, el tiempo se divide en ranuras discretas cuya longitud es de  $2\tau$  en el peor de los casos que equivalen a 51.2  $\mu$ seg. Tras la primera colisión, cada estación espera 0 a 1 tiempos de ranura antes de intentarlo de nuevo, después de la segunda colisión, cada estación escoge 0,1, 2 ó 3 ranuras de tiempo al azar y espera ese número de tiempos de ranura, si ocurre una tercera colisión, entonces para la siguiente vez el número de ranuras a esperar se escogerá al azar del intervalo  $2^3 - 1$ , esto se puede generalizar con la siguiente ecuación:

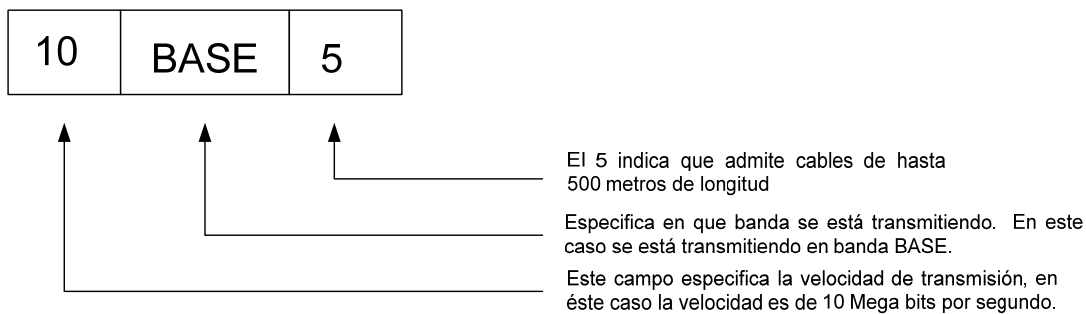
$$RP = 2^i - 1$$

Donde RP es ranuras posibles de espera e i es el número de colisiones, entonces una estación escoge al azar una de las RP. Este algoritmo es llamado retroceso exponencial binario. Este algoritmo asegura un retardo pequeño cuando pocas estaciones colisionan, pero además asegura que la colisión sea resuelta en un tiempo razonable cuando existen colisiones entre muchas estaciones.

Ethernet es una topología de bus lógica pero físicamente es una topología en estrella, pues la distribución física del cableado es como una estrella, donde el concentrador puede ser un hub o un switch. Ethernet utiliza diferentes tipos de medios físicos para transmitirse, dentro de los cuales el más utilizado en la actualidad es el cable UTP (*Unshielded twisted pair*) categoría 5e. Otros de los medios de transmisión que se utilizó mucho a principio del año 1980 fue el cable coaxial grueso y delgado.

Para cada una de estos sistemas de cableado utilizados en ethernet IEEE 802.3, el comité 802.3 adoptó una norma con la cual se le asigna un nombre a cada uno de estos sistemas. El nombre iba a estar constituido por tres partes, esto se ejemplifica mejor en la figura 14.

**Figura 14. Especificación de norma según medio utilizado**



Las diferentes normas que existen para ethernet son la 10BASE5, 10BASE2 y la 10BASET.

La norma IEEE 802.3 10BASE 5, se originó a principio de la década de los 80's, transmitía a 10 Mbps sobre un cable coaxial grueso en topología de bus, éste fue el primer medio que se utilizó en ethernet. El principal beneficio de esta norma era la longitud pues se podía tener cables de longitud de hasta 500 metros sin necesidad de amplificar o rectificar la señal. 10BASE5 hace uso de la codificación Manchester. 10BASE5 es la que se utiliza en la mayoría de redes con topología en bus o árbol. A este tipo de red se le denominó ethernet thicknet, debido al cable coaxial grueso. Este tipo de red se dejó de utilizar debido al grueso del cable, pues era muy difícil de instalar y manejar, además que sólo transmitía en half-duplex.



La norma IEEE 802.3 10BASE2 se introdujo en el año 1985, su instalación era más sencilla debido a su menor tamaño, peso y flexibilidad. Este tipo de tecnología utiliza cable coaxial pero de menor diámetro, es por ello que se le denominó thinnet. También transmite a 10 Mbps en banda base, pero la longitud máxima del cable es de 185 metros que se aproximan a 200. Esta topología lógica es la que se utiliza en las redes con topología física de bus o árbol.

La norma 10BASET es la más utilizada en la actualidad, fue introducida en el año de 1990. Esta transmite siempre a 10 Mbps en banda base pero el medio físico de transmisión se hace sobre un cable de cobre de par trenzado no blindado (UTP), el cual es más económico y más fácil de instalar y manejar. Este tipo de tecnología se instala en topología física de estrella, aunque lógicamente es un bus. También utiliza codificación Manchester. La “T” viene de “twisted” que en español significa trenzado. La longitud máxima del cable es de 90 metros. Este tipo de cable utiliza un conector tipo RJ-45 (*Registered Jack – 45*) de ocho pines. Los cuatro pares de pines se pueden utilizar con la disposición T568A o bien con la T568B. La disposición de los pines en un conector RJ-45 se muestra en la siguiente tabla:

**Tabla I. Disposición de pines en un conector RJ-45**

Número de pines	Señal
1	TD+ ( Transmitir datos, señal positiva )
2	TD- (Transmitir datos, señal negativa)
3	RD+ (Recepción de datos, señal positiva)
4	Sin usar
5	Sin usar
6	RD- (Recepción de datos, señal negativa)

7	Sin usar
8	Sin usar

#### 1.1.2.2.1.2 Fast ethernet

Fastethernet no es más que uno de los pasos dado en la evolución de ethernet, pues tal y como su nombre lo indica es ethernet rápida, el estándar es el IEEE 802.3u y fue aprobado en junio de 1995. Ethernet es una topología lógica en la cual su velocidad de transmisión era de 10 Mbps como máximo. Fastethernet es un protocolo que permite transmisión de datos a 100 Mbps como máximo. El medio físico por el que se transmite es UTP para 100BASE-TX, pero además también se utiliza la fibra óptica para 100BASE-FX. La trama es igual a la trama ethernet anteriormente descrita. Fastethernet transmite 10 veces más rápido que ethernet, por ello hay que tener mayor cuidado porque los bits enviados se acortan en duración y se producen con mayor frecuencia, como resultado son más susceptibles al ruido. A consecuencia de lo anterior se decidió utilizar dos pasos para la codificación, la primera utiliza la técnica denominada 4B/5B, y la segunda es la codificación real de la línea especificada para el cobre. Los parámetros de fastethernet son los siguientes, el período de bit es de 10 ns, una ranura temporal de 512 un bit o 64 bytes, un espacio entre tramas de 96 bits, y un tamaño máximo de trama sin rotular de 1518 octetos.

100BASE-TX es el estándar de fastethernet la cual se transmite en un medio de cobre que es el cable UTP categoría 5e. La transmisión a full duplex permite que más de una estación transmitiera a la vez, cuando transmite a half duplex transporta 100 kbps y cuando lo hace a full duplex transporta 200 kbps. Utiliza una codificación 4B/5B que luego es mezclada y convertida a 3 niveles de transmisión de multinivel MLT-3. La disposición de pins en el conector RJ-

45 es el mismo que para ethernet, o sea que sólo se utilizan dos cables de par trenzado, uno para transmitir y otro para recibir.

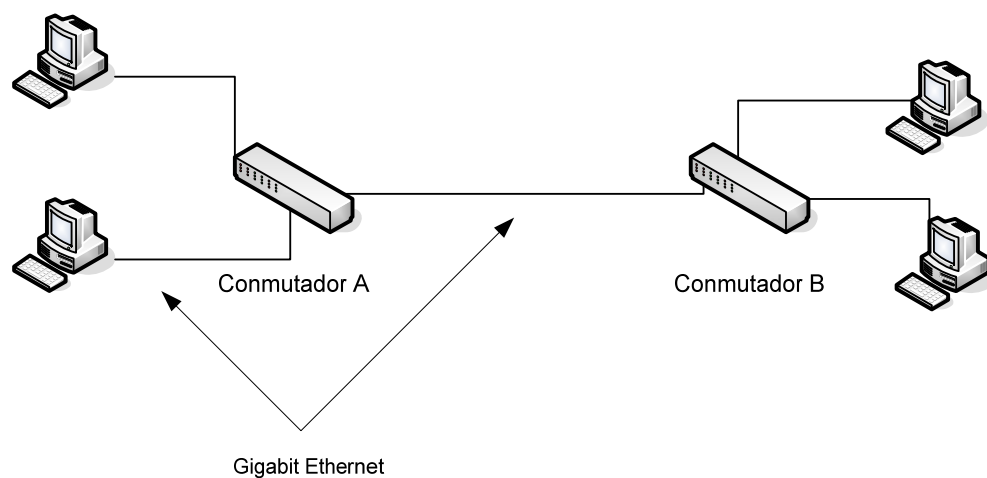
100BASE-FX es una versión de fastethernet utilizando como medio de transmisión dos filamentos de fibra óptica multimodal, una para cada dirección, y que se utiliza especialmente para backbones, conexiones entre distintos edificios y donde existe más ruido en los cuales el cobre no es aconsejable. No tomó mucho éxito debido a que Gigabitethernet se introdujo también. La temporización el formato de la trama y la transmisión son las mismas que la que utiliza la versión de cobre, la única diferencia, es la codificación que se utiliza en la versión para fibra, pues se utiliza NRZI. La distancia máxima entre una estación y un conmutador es de 2 kilómetros. Se menciona conmutador pues no es posible utilizar concentrador, pues los cables 100BASE-FX son muy largos para el algoritmo de colisiones por lo que se utiliza un conmutador en el cual cada trama entrante se almacena en el búfer de una tarjeta de conexión y se pasa a través de una matriz de conmutación de alta velocidad de la tarjeta origen a la de destino.

#### **1.1.2.2.1.3 Gigabit Ethernet**

Gigabit ethernet se comenzó a diseñar al poco tiempo de haber terminado el estándar fastethernet, y se terminó y aprobó por el IEEE en 1998 bajo el nombre de 802.3z. La “z” se originó pues se pensaba que ya no iba a haber otra versión más rápida, pues la z es la última letra del abecedario. Esta al igual que fastethernet, también es un paso más en la evolución de ethernet, pues es 100 veces más rápida que ethernet. La velocidad máxima de transmisión es de 1 gigabit por segundo (1 Gbps). Gigabit ethernet soporta dos modos de transmisión, half duplex y full duplex, de los cuales el más utilizado es el full duplex. El modo full duplex se utiliza cuando se tiene un conmutador

central al cual están conectadas todas las estaciones, entonces las estaciones no necesitan el protocolo CSMA/CD pues no necesitan escuchar el medio antes de transmitir. Se dice que no necesitan escuchar pues la estación es la única que está conectada a través de ese cable en particular a una tarjeta del conmutador (existe otro tipo de tarjeta para conmutadores en donde no existe buffer, en donde si es necesario CSMA/CD), entonces no va a existir colisiones pues la otra parte que pudiera estar transmitiendo sería el concentrador hacia la estación, pero como es full-duplex entonces puede transmitir y recibir datos simultáneamente. Esto se ejemplifica mejor en la figura 15, en la cual se puede observar la distribución de las estaciones y los conmutadores.

**Figura 15. Red Gigabit ethernet utilizando conmutadores**



En la figura 15 se observa estaciones conectadas a un conmutador, estas estaciones pueden estar conectadas a la misma tarjeta o a distinta tarjeta, el uso de CSMA/CD va a depender del tipo de tarjeta del conmutador. Entonces cuando una estación desea transmitir envía los datos sobre el cable hacia la tarjeta del conmutador, donde es almacenado en el buffer (si es la tarjeta que no utiliza CSMA/CD) de la tarjeta, la tarjeta verifica si el destino está conectado

en otro puerto de ella o está en otra tarjeta, si estuviera conectada en otro puerto la envía directamente, si estuviera en otra tarjeta entonces utiliza la matriz de conmutación para enviarla a la otra tarjeta.

Se utiliza el modo half duplex cuando se conectan las estaciones a un concentrador o hub. El concentrador no tiene buffer para almacenar las tramas entrantes, el concentrador conecta en forma eléctrica todas las líneas internamente, simulando el cable con múltiples derivaciones. Por lo anterior en este tipo de modo sí es necesario la utilización del protocolo CSMA/CD. Dado a que una trama mínima de 64 bytes ahora se transmite 100 veces más rápido que la IEEE 802.3 la distancia mínima se reduce a 25 metros, con lo cual se asegura que el emisor no haya terminado de transmitir cuando la ráfaga de ruido regrese a él. Los 25 metros de radio fueron inaceptables, con lo cual el comité decidió agregarle dos características al estándar para incrementar el radio. La primera se llamó extensión de portadora, la cual consiste en que el hardware le agregue o rellene la trama para llegar a 512 bytes, pero la eficiencia de la línea baja a el 9% pues es utilizar un ancho de banda de 512 bytes para transmitir 46 bytes de datos de carga útil de usuario. La segunda opción se llamó ráfagas de trama, la cual permitía que un emisor transmitiera una secuencia concatenada de múltiples tramas en una sola transmisión. Si aún así la ráfaga total era menor que 512 bytes entonces se rellenaba por el hardware. Esta segunda opción era más eficiente si suficientes tramas esperan la transmisión, y se prefería antes que la primera. Con estas nuevas características el radio se amplió a 200 metros, lo cual ya es aceptable para la mayoría de oficinas.

La tabla II muestra las versiones del protocolo Gigabit ethernet que existen dependiendo del medio en el cual se transmiten y las longitudes que cubren los mismos.

**Tabla II. Versiones de Gigabit Ethernet según el medio de transmisión**

<b>Nombre</b>	<b>Medio de TX</b>	<b>Longitud maxima</b>	<b>Ventajas</b>
1000BASE-SX	Fibra óptica	550 metros	Multimodo (50, 62.5 micras)
1000BASE-LX	Fibra óptica	5000 metros	Monomodo (10 $\mu$ ) o multimodo (50, 62.5 $\mu$ )
1000BASE-CX	2 pares de STP	25 metros	Cable de par trenzado blindado
1000BASE-T	4 pares de UTP	100 metros	UTP Cat 5e

Fuente: Andrew S. Tanenbaum. Pagina 288.

Como se observa en la tabla II, gigabit ethernet permite transmitir en fibra óptica y en cable de cobre. Para transmitir en fibra óptica el emisor debe de ser un láser pues un led no puede funcionar a la frecuencia de 1 nano segundo que es la frecuencia a la que se transmiten un bit en gigabit ethernet . Los láser pueden utilizar dos longitudes de onda, la de 0.85 micras y la de 1.3 micras.

El tipo de codificación que utiliza Gigabit ethernet en fibra es la llamada 8B/10B que se basa en un canal de fibra donde cada byte de 8 bits está codificado en 10 bits y debido a que hay  $2^{10} = 1024$  palabras codificadas posibles para cada byte de entrada, existe cierta libertad para elegir cuales se van a permitir, es por ello que se crearon unas reglas bajo las cuales se eligen, la primera es que ninguna palabra codificada podría tener más de cuatro bits idénticos en una fila, y la segunda es que ninguna palabra codificada podría tener más de seis bits 0 o seis bits 1. Con estas elecciones se lograba mantener un equilibrio de 1 y 0 con lo cual se obtiene un componente DC bajo en la señal transmitida.

El siguiente paso del protocolo ethernet es 10 Gigabit ethernet que fue establecida en junio de 2002 por IEEE bajo el nombre de IEEE 802.3ae. 10 Gigabit ethernet puede alcanzar longitudes de hasta 40 kilómetros, con lo cual ethernet deja de ser un protocolo utilizado para LAN y se comienza a utilizar en MAN y WAN como una compatibilidad con la red óptica síncrona (SONET) y con redes síncronas de jerarquía digital (SDH). El formato de la trama de 10 Gigabit ethernet es el mismo que Gigabit ethernet que Fast ethernet y ethernet, pues como se mencionó antes, ethernet es una tecnología escalable o sea que es compatible con sus versiones anteriores. En 10 Gigabit ethernet el tiempo de bit es 0.1 nano segundo, como se utiliza transmisiones full duplex no es necesario CSMA/CD.

10 Gigabit ethernet utiliza únicamente como medio de transmisión la fibra óptica monomodo y multimodo. Aquí no existen colisiones pues opera en full duplex, el tamaño mínimo de la trama es de 64 bytes. Debido a la frecuencia de transmisión de bits, que es mucho mayor, esto trae como consecuencia mayor susceptibilidad al ruido pues dado a que el bit dura muy poco (0.1 nseg), es muy difícil separa el bit del ruido. Por esto es que en 10 Gigabit ethernet se utilizan dos pasos en la codificación.

10 Gigabit ethernet también tiene diversas versiones dependiendo de la longitud que se quiera abarcar y del medio de transmisión a utilizarse. Las diferentes versiones que existen son, 10GBASE-SR, 10GBASE-LX4, 10GBASE-LR, 10GBASE-ER, 10GBASE-SW, 10GBASE-LW y 10GBASE-EW. 10GBASE-SR utiliza fibra multimodo y cubre una distancia entre 26 y 82 metros. 10GBASE-LX4 admite un distancia entre 240 a 300 metros utilizando fibra multimodo y utilizando fibra monomodo 10 kilómetros. 10GBASE-LR y 10GBASE-ER admiten distancias de 10 a 40 kilómetros en fibra monomodo.

10GBASE-SW, 10GBASE-LW y 10GBASE-EW su objetivo es ser compatibles con SONET y SDH.

#### **1.1.2.2.2 Determinísticas**

En esta topología lógica se debe de esperar turnos para que una estación pueda transmitir, a diferencia de las no determinísticas que el primero que escucha libre el medio es el que transmite. Cada estación debe de esperar su turno de poder transmitir, y esto se controla por medio de un testigo o token, el testigo circula por todo el anillo o circuito cerrado, el token es tomado por una estación y esta estación es la única que va a poder transmitir en ese momento, las demás estaciones que conforman la red deben de esperar su turno (cuando posean el token) para poder transmitir. Existen diversas formas que una estación pueda obtener el token y esto va a depender de que topología determinística se esté utilizando. Existen dos topologías determinísticas, token ring y FDDI.

##### **1.1.2.2.2.1 Token Ring**

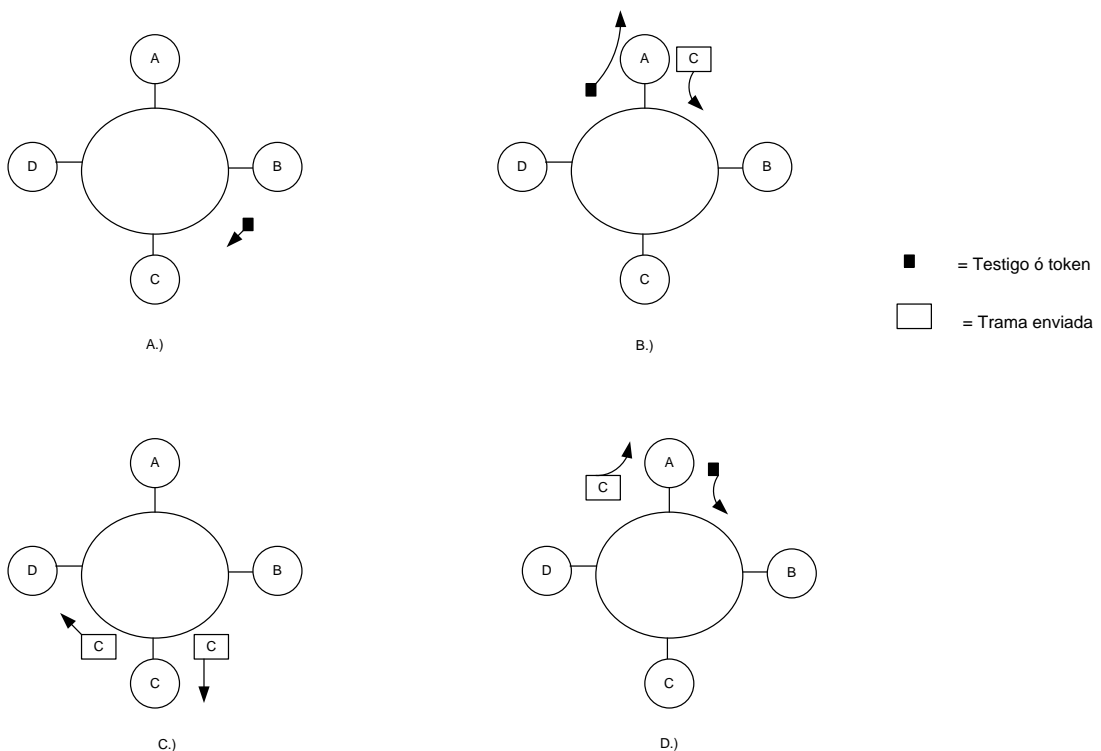
Esta topología fue desarrollada por IBM y cedida a la IEEE quienes la estandarizaron y la denominaron IEEE 802.5. Se le denomina token ring o anillo de señales en español, pues lógicamente esta red está constituida como un anillo, dado a que el método de acceso y el recorrido de la trama avanza de una estación a otra y de ésta a otra y así sucesivamente hasta cerrar el circuito. Físicamente, la forma de conexión de esta red es la de una estrella, pues cada una de las estaciones parte de un punto central.

Esta red está basada en el paso de un testigo o token, la cual es una pequeña trama que circula cuando todas las estaciones están libres, o sea



cuando ninguna está transmitiendo. Si una estación desea transmitir debe de esperar hasta cuando posea el testigo y así poder trasmitir, entonces las demás estaciones solamente deben de escuchar y esperar hasta que la estación termine de transmitir y nuevamente esté el testigo circulando y alguna otra estación pueda tomarlo para transmitir. El testigo circula por todo el anillo, es tomado por la estación transmisora y es generado por ésta misma cuando termina de transmitir. El testigo puede ser generado únicamente cuando la estación transmisora haya recibido los bits iniciales de la trama transmitida, o si el anillo es muy grande, cuando haya terminado de transmitir. El funcionamiento de token ring se ilustra en la figura 16.

**Figura 16. Funcionamiento de token ring**



En la figura 16.a el testigo o token está circulando por el anillo, en la figura 16.b el testigo es tomado por la estación A, pues ésta desea transmitir un paquete a la estación C, el paquete se genera y es enviado a C, en la figura 16.c la estación C copia el paquete que es dirigido hacia ella y lo reenvía, en la figura 16.d la el paquete vuelve a la estación que lo originó donde es drenado y eliminado a la misma vez que la estación A genera el testigo para que otra estación tenga la oportunidad de transmitir. Este proceso es el que se lleva a cabo cuando una estación transmite en una red token ring.

En una red token ring, la trama a nivel de la capa de acceso al medio del modelo osi, consta de varios campos los cuales se muestran en la figura 17.

**Figura 17. Formato de una trama token ring**

SD (1)	AC (1)	FC (1)	DA (6)	SA (6)	UNIDAD DE DATOS (≥0)	FCS (4)	ED (1)	FS (1)
-----------	-----------	-----------	-----------	-----------	-------------------------------	------------	-----------	-----------

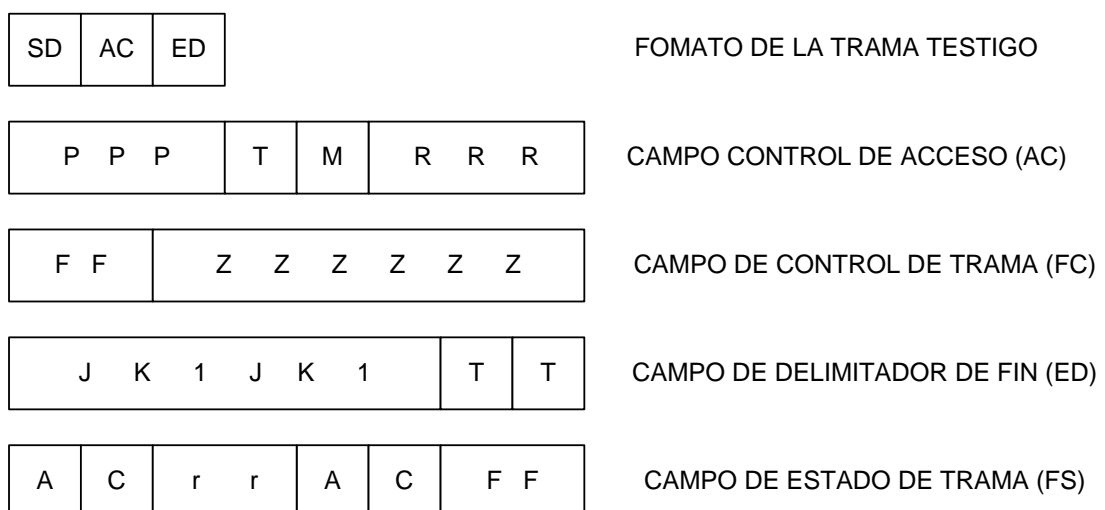
( ) = Número de octetos

Fuente: William Stallings, página 451

El campo delimitador de comienzo (SD), está compuesto por un byte, este campo indica el inicio de la trama y el patrón se codifica como JK0JK000, donde J y K son símbolos que representan no datos. El campo control de acceso (AC) también está compuesto por un byte, este campo se utiliza para manejar la prioridad y reserva, esto lo hace por medio del manejo de 3 bits P, 3 bits R, el bit T y el bit M. El bit T indica si es una trama de datos o es una trama de testigo, el bit M es el bit monitor, los bit P son los bits de prioridad y los bits R son los bits de reserva.

El campo de control de trama (FC) indica si la trama es datos de control de enlace lógico, de no serlo controlan el protocolo MAC, esto lo hace por los bits F que indican bits de tipo trama y los bits Z que indican bits de control. El campo dirección destino (DA) y el de dirección origen (SA) contienen las direcciones MAC correspondientes de origen y destino. El campo de unidad de datos contiene los datos de la capa de control de enlace. El campo de la secuencia de comprobación de trama (FCS), al igual que en ethernet, es la encargada de verificar los errores en la secuencia de las tramas. El campo delimitador de fin (ED), que contiene el bit E que se utiliza si algún repetidor detectó error, además también contiene el bit intermedio I el cual si está activado indica que la trama no es la última trama de la transmisión. El campo de estado de trama (FS), contiene los bits de trama copiada (C) y el de dirección reconocida (A), estos bits están duplicados pues no están cubiertos por el campo FCS, además contiene los bits r de reservado. Cada uno de estos campos se desglosa en la figura 18.

**Figura 18. Detalle de los campos de una trama token ring**



Fuente: William Stallings, página 451

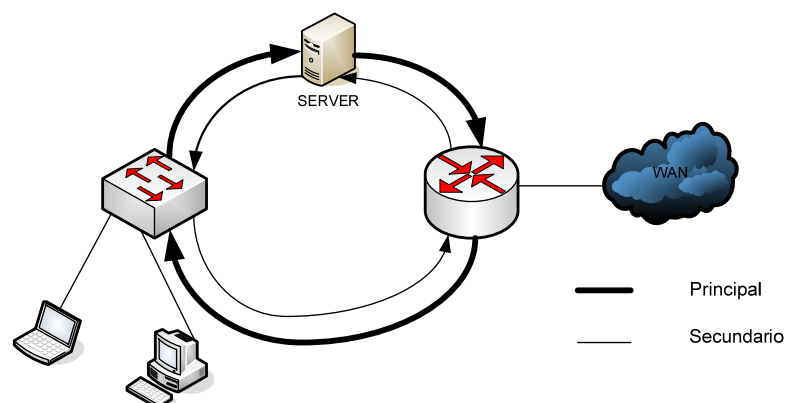
Cuando una estación desea transmitir debe esperar la trama testigo la cual debe tener desactivado el bit T del campo AC, la estación toma la trama y activa el bit T, entonces los campos SD y AC se convierten en campos de una trama transmitida. Cuando la estación termina de transmitir o el contador de posición de testigo expira, la estación desactiva el bit T y añade el campo ED, con lo cual se forma un nuevo testigo para que otra estación lo pueda tomar y transmitir.

Como se mencionó en el campo AC existen unos bits P y R que son para prioridad y reserva respectivamente. Los niveles de prioridad son 8, pues son 3 bits para cada campo ( $2^3 = 8$ ). Cuando una estación desea transmitir, puede reservar la trama si la estación tiene una prioridad mayor a la reserva de la trama actual, lo único que tiene que hacer es reservar el siguiente testigo con su nivel de prioridad mientras pasa la trama, con esto el siguiente testigo debe tener el nivel de prioridad reservado y las otras estaciones que quieran tomar el testigo para poder transmitir no podrán si tienen un nivel de prioridad menor que la prioridad del testigo, entonces el testigo se dirige a la estación que lo había reservado y la estación puede comenzar a generar sus tramas de datos. Por ejemplo, una estación A está transmitiendo datos a una estación B con nivel de prioridad 0, entonces una estación D hace una reserva con prioridad 3 ( $R=3$ ), cuando la trama de datos termina la vuelta en el anillo y retorna a A, A genera un testigo con prioridad igual a 3. Si ninguna otra estación tiene prioridad igual a 3 o mayor, entonces la estación D toma el testigo y comienza su transmisión de datos. Una vez terminada la transmisión de datos de la estación D, ésta genera un testigo con prioridad igual a 3 (si ninguna otra estación había reservado con un nivel mayor), entonces cuando la estación A detecta el testigo con prioridad 3 lo toma (aunque no tenga que transmitir datos) y genera un testigo con el nivel de prioridad anterior ( en este caso el nivel prioridad inicial era 0 ), con esto se completa un proceso en una red con topología Token Ring.

### 1.1.2.2.2 FDDI

FDDI (*Fiber Distributed Data Interface*) o interfaz de datos distribuidos por fibra, es un esquema de anillo parecido a la especificación Token ring, pero que fue diseñado para aplicaciones LAN y MAN y que además lógicamente es un anillo pero físicamente está cableado como anillo doble, a diferencia de Token ring que físicamente está cableado como una estrella. Esta surgió con una velocidad de 100 Mbps a través de un anillo dual, surgió debido a las limitaciones de distancia que sufría ethernet. FDDI es utilizada comúnmente como backbone (espina dorsal o parte principal de una red), debido a que soporta grandes anchos de banda y mayores distancias que el cobre. FDDI utiliza una arquitectura de dos anillos por los cuales circula información en direcciones opuestas. Los anillos se denominan Primario y Secundario. En una transmisión normal se utiliza el Primario para transmitir, mientras el secundario está en inactividad, la configuración de doble anillo se utiliza para darle confiabilidad y robustez. En la figura 19 se puede observar una red con topología FDDI.

**Figura 19. Ejemplo de una red utilizando topología FDDI**



El medio principal de transmisión que utiliza FDDI es la fibra óptica por todas sus ventajas, pero también utiliza el cobre o CDDI (*Cooper Distributed Data Interface*). Cuando se utiliza fibra, puede alcanzar hasta 2 kilómetros entre estaciones utilizando fibra multimodo y distancias más largas si se utiliza fibra monomodo.

En FDDI se pueden conectar cuatro tipos de dispositivos que son: SAS (*Single Attachment Station* o estación de una sola conexión), DAS (*Dual Attachment Station*), SAC (*Single Attachment Concentrador* o concentrador de una sola conexión) y la última DAC (*Dual Attachment Concentrator*). Un dispositivo SAS se conecta sólo al anillo primario a través de un concentrador, y ésta no tendrá ningún efecto sobre el anillo si se desconecta y se apaga. Los dispositivos DAS tienen dos puertos A y B que conectan el dispositivo a las dos partes del anillo, en este tipo de dispositivo importa si se desconecta o si se apaga como se verá más adelante. El dispositivo DAC es el concentrador que logra unir las dos partes del anillo y es por medio del cual se logran conectar los SAS al anillo y quién asegura que la falta de energía en un SAS no interrumpa el anillo, esto es particularmente útil cuando se conectan computadoras personales que se encienden y se apagan con frecuencia.

Una de las características de FDDI es que tolera varias faltas o problemas que se puedan dar en el anillo y aún así poder continuar trabajando. La primer característica de este tipo es el Anillo doble, si una estación conectada en el anillo doble se apaga o el cable con el que se conecta se daña, automáticamente el anillo se cambia al modo anillo simple y los datos siguen fluyendo. Se ha de remarcar que el anillo no se interrumpe si hubo un problema en un solo punto, pero si existen más de dos puntos que tuvieron problemas simultáneamente el anillo se verá interrumpido.

La segunda característica para la corrección de problemas se le denomina interruptor de puente óptico (*OB Optical Bypass*), esto se utiliza para eliminar la segmentación del anillo cuando una SAS se apaga. Esta característica se logra por medio de la utilización de unos espejos ópticos que se colocan antes de la estación DAS, y en la operación normal, el espejo deja pasar directamente la luz hacia la estación pero cuando se presenta un problema en dicha estación, el espejo dirige la luz por donde vino, o sea que ya no permite que continúe hacia la estación DAS y con esto no se interrumpe el anillo.

La trama MAC se compone de los siguientes campos, preámbulo, delimitador de comienzo (SD), control de trama (FC), dirección destino (DA), dirección origen (SA), secuencia de comprobación de trama (FCS), delimitador de fin (ED), y estado de trama (FS). La trama de un testigo se compone únicamente de los campos preámbulo, SD, FC, y ED. En la figura 20 se ilustra los formatos de los dos tipos de tramas.

**Figura 20. Formato de una trama genérica FDDI y de un testigo.**

Preámbulo ( 64)	SD (8)	FC (8)	DA (16 o 48)	SA (16 o 48)	Info (0)	FCS (32)	ED (4)	FS (12)
--------------------	-----------	-----------	-----------------	-----------------	-------------	-------------	-----------	------------

( ) = Número de bits

A.) Formato de una trama genérica

Preámbulo ( 64)	SD (8)	FC (8)	ED (4)
--------------------	-----------	-----------	-----------

B.) Formato de un testigo

Fuente: William Stallings, página 456

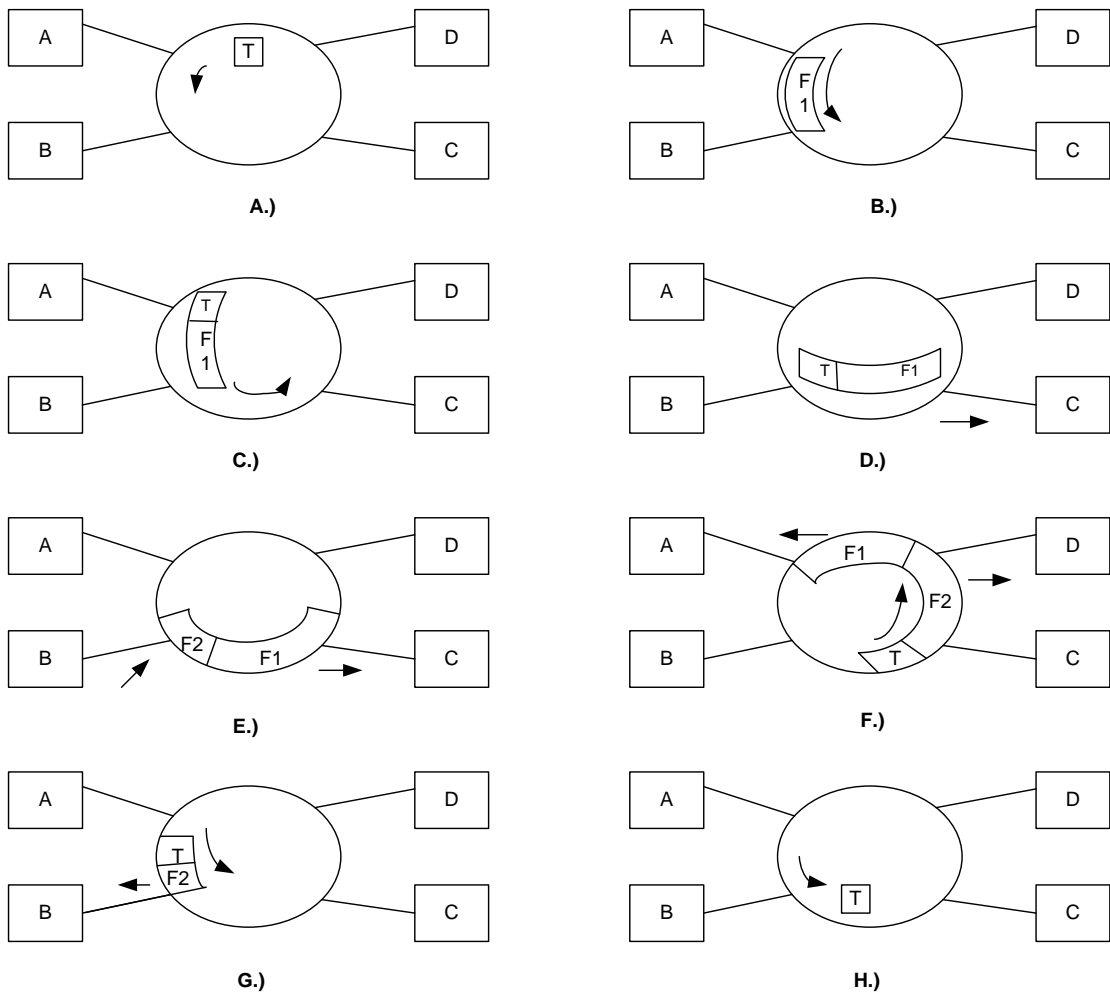
El campo preámbulo es la encargada de la sincronización de la trama con el reloj de la estación, la estación emisora utiliza un campo de 16 símbolos de no datos (cada símbolo equivale a 4 bits). El campo SD, como su nombre lo indica, indica el comienzo de una trama y los símbolos que presenta son J y K. El campo de FC, tiene el formato de bits CLFFZZZZ, donde FF indica si es una trama LLC, MAC o reservada, el bit C indica si es una trama síncrona o asíncrona, el bit L indica el uso de direcciones de 16 o de 48 bits. Los campos dirección destino y origen indican la dirección física o MAC destino y origen, respectivamente. El campo FCS es el que se utiliza para verificar los errores por medio de la comprobación de redundancia cíclica (CRC) referente a los campos FC, DA, SA y de información. El campo delimitador de final, contiene un símbolo de no datos y marca el fin. En el campo FS están contenidos los indicadores, al igual que en token ring, E que indica la detección de un error en la trama, A que indica dirección reconocida y por último el indicador C que indica cuando una trama ha sido copiada.

Con respecto a los campos de un testigo, el campo preámbulo y SD se describen igual que una trama genérica, el formato del campo FC presenta bits 10000000 ó 11000000 para indicar que es un testigo. El campo ED utiliza un símbolo de no datos T para indicar el fin de la trama.

El funcionamiento de este protocolo es muy similar al protocolo IEEE 802.5 pero con algunas variaciones, como por ejemplo en FDDI el testigo es transmitido inmediatamente después de haber terminado de transmitir los datos la estación emisora, aún cuando no hayan regresado a ella. Otra diferencia remarcable es que cuando una estación toma el testigo, lo absorbe y no lo repite, crea un nuevo testigo únicamente cuando ha terminado de enviar la trama de datos. El funcionamiento del protocolo FDDI se ilustra en la figura 21.



**Figura 21. Ejemplo del funcionamiento de una red con FDDI**



Fuente: William Stallings, página 458

En la figura 21.a se observa que la estación A está esperando un testigo para poder transmitir, en 21.b la estación A ya tomó el testigo y la elimina además emite su trama de datos dirigida a la estación C. En la figura 21.c se observa que A terminó de emitir su trama de datos e inmediatamente genera su testigo, en la figura 21.d la estación C comienza a copiar la trama mientras circula. En la figura 21.e la estación C continúa copiando la trama F1 que le

envió la estación A, mientras que la estación B toma el testigo lo elimina e inmediatamente comienza a transmitir su trama de datos F2 dirigida hacia la estación D. En la figura 21.f la estación B termina de emitir su trama por lo que genera su testigo, además la estación D comienza a copiar la trama F2 mientras circula, y la estación A comienza a absorber la trama F1 que había enviado con anterioridad. En la figura 21.g la estación B comienza a absorber la trama F2 y deja pasar el testigo. En la última figura se puede observar que el testigo sigue circulando en el anillo debido a que no hay en ese momento ninguna estación que desee transmitir y así seguirá circulando hasta que haya alguna estación que quiera transmitir y tome el testigo.

## 2. ANALISIS DEL PROTOCOLO ACTUAL IPv4

Actualmente aún se continúa utilizando el protocolo enrutado IP versión 4, pues aunque ya se estén acabando las direcciones ip públicas, y muchos administradores de redes acudan a utilizar sub-redes y a utilizar las direcciones ip privadas de las cinco clases que existen, IPv4 aún sigue siendo bastante funcional mientras las redes se comienzan a migrar a IPv6.

Para poder entender bien el nuevo protocolo IP versión 6, se dará una breve introducción de la versión anterior de este protocolo enrutado. Es por ello que en los inicios de este capítulo también se tratará con el modelo de referencia OSI (*Open System Interconnection* o Interconexión de sistemas abiertos), pues es un modelo que como su nombre lo indica, nos sirve como referencia para otros modelos.

### 2.1 Modelo de referencia OSI

Dado que la comunicación entre una estación y otra estación es un proceso que si se ve como uno solo, sería muy complejo de poder entender como funciona. Es por ello que se establecen capas para poder entender de una mejor manera como se establece paso a paso la comunicación entre estaciones.

El modelo OSI es un modelo de referencia propuesto por la ISO (Organización Internacional de Estándares) como resultado de la necesidad de poder tener un estándar para los distintos protocolos que a principios de los años 80 comenzaron a crecer rápidamente. El modelo OSI fue lanzado en el

año 1984 y proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad entre los distintos tipos de tecnología de red. El modelo OSI es un modelo que tiene 7 capas, las cuales van desde el medio físico por el que se transmiten los datos, hasta la parte de las aplicaciones, que son con las cuales el usuario tiene interactividad.

Las 7 capas de este modelo se ilustran en la figura 22.

**Figura 22. Capas del modelo de referencia OSI**

7. Aplicación
6. Presentación
5. Sesión
4. Transporte
3. Red
2. Enlace de datos
1. Física

Cada una de estas capas se crearon cumpliendo con las siguientes características, una capa se crea donde se necesita una abstracción diferente, cada capa realiza una función bien definida, dicha función se elige con la intención de definir protocolos estandarizados internacionalmente, cada capa debe tener un límite con el objeto de minimizar el flujo de información y por último, el número de capas debe ser lo suficientemente grande para que en una misma capa no hayan muchas funciones, ni demasiado pequeña para que la arquitectura sea muy compleja e inmanejable. En otras palabras, se puede

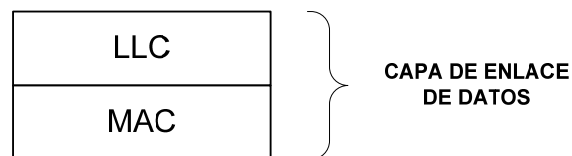
decir que el modelo OSI es un marco que se utiliza para comprender como viaja la información a través de una red.

La capa física, en ésta el pdu (*packet data unit*) son los bits, pues es en esta capa donde se lleva a cabo la transmisión y recepción de los bits, a través de los distintos medios físicos. Los bits pueden tomar valores 1 ó 0 (sistema binario), y éstos pueden ser representados por variaciones en las señales, esto quiere decir que un 0 lógico se puede representar por medio de un nivel de voltaje específico. Se utiliza una gran variedad de medios en la comunicación de datos, cables eléctricos, fibras ópticas, ondas de radiofrecuencia, ondas de microondas, etc. El medio empleado se puede variar y basta con sustituir el protocolo de capa física para poder cambiarlo. Entonces en esta capa es donde se consideran los voltajes, los cables y los conectores. Por ejemplo, en esta capa es donde se sitúan los tipos de interfaces que existe, como por ejemplo la interfaz serial V.35 y RDSI (Red Digital de Servicios Integrados) para enlaces WAN, la interfaz Ethernet para enlaces LAN, etc.

La capa de enlace de datos es la encargada de hacer seguro el medio físico que proporciona la anterior capa. La pdu de esta capa es denominada "Trama", pues los bits que se tienen en la capa física se agrupan de tal manera que a estos grupos se les denomina tramas. La capa de enlace se encarga de la detección y control de errores en la transmisión de las tramas. El entramado es necesario pues sólo las corrientes de bits no eran suficientes para establecer una comunicación. En la trama viaja información como por ejemplo cuáles son las computadoras que se comunican entre sí, cuándo comienza y cuándo termina la comunicación, el control de errores y quién tiene el turno para poder transmitir entre otros. Podemos ver entonces que es en esta capa donde se sitúan los protocolos ethernet, token ring y FDDI que tratamos en el capítulo 1, con esto se puede decir entonces que ethernet es un protocolo de capa 2 del

modelo OSI. Un ejemplo de una trama es la trama IEEE 802.3 explicada en el capítulo anterior. La capa de enlace es la única capa del modelo OSI que se subdivide en otras dos subcapas, estas subcapas son la subcapa LLC (*Link Layer Control* o capa de enlace de control) y la subcapa MAC (Media Access Control o control de acceso al medio). La figura 23 muestra la división de la capa de enlace de datos.

**Figura 23. Subdivisión de la capa de enlace de datos**



La subcapa MAC es la que trata con los componentes físicos que se utilizarán para la comunicación. Cada uno de los protocolos de la capa de enlace de datos, utilizan direcciones MAC también conocidas como direcciones físicas, pues es una dirección que se le asigna a la tarjeta de red o NIC (*Network Interface Card*), tal y como se indicó en el anterior capítulo.

La subcapa LLC proporciona una interfaz de red para los protocolos de capas superiores, es decir toma los datos de la capa superior, por ejemplo los datos provenientes de un protocolo enrutado ip y agrega información de control para ayudar en la entrega de ese paquete a un nodo que está asociado a su NIC por medio de la dirección MAC. Esta subcapa es la encargada de la recuperación de tramas erradas, esto quiere decir que la subcapa MAC detecta los errores y LLC es quien las corrige por medio de los acuses de recibido y de la solicitud de repetición automática o ARQ (*Automatic Repeat Request*).

Continuando con las capas del modelo OSI, la capa 3 o capa de red es la encargada de poder escoger la mejor ruta que existe para ir de un punto hacia otro punto, conmutar y encaminar los paquetes y además de poder direccionar o asignar una dirección lógica a una estación. Esta dirección lógica se le denomina dirección IP (*Internet Protocol*). Los protocolos que trabajan en esta capa son, el protocolo enrutado IP del cual trata este trabajo, protocolo de Internet de control de mensajería o ICMP, el protocolo enrutado IPX y otros. Esta capa tiene relación directa con la subcapa LLC de la capa de enlace de datos. La pdu de esta capa es el datagrama o como comúnmente se le denomina paquete. En esta capa aparecen las redes y subredes y es aquí donde se puede dividir el dominio de broadcast (o difusión). Cuando se recibe mensajes de las capas inferiores, la capa de red añade una cabecera al mensaje que incluye las direcciones ip origen y destino, y otros campos más que se detallarán más adelante, y forman el paquete o datagrama. El proceso de hacer llegar los paquetes a la red correcta se denomina encaminamiento (*routing* en inglés). El router o encaminador es el dispositivo que trabaja en esta capa, y éste hace la selección de la mejor ruta a través de tablas de enrutamiento dinámicas o estáticas, que son características del protocolo de enrutamiento que el encaminador utilice. Para poder hacer el encaminamiento, la capa de red debe conocer la topología de la red y de las subredes, a esto es lo que se le denomina tablas de enrutamiento. Esta capa también es responsable de controlar la calidad de servicio y las características como retardo, tiempo de tránsito e inestabilidad.

La capa de transporte es una capa la cual tiene como función básica aceptar los datos de las capas superiores y dividirlos en segmentos (segmento es el pdu de esta capa) que coincidan con el límite de tamaño de la red, pasar los segmentos a la capa de red y asegurarse de la entrega de cada uno de estos segmentos. Cada uno de los segmentos debe de tener un tamaño

específico dependiendo de la red, este tamaño específico se denomina MTU (*Maximum Transfer Unit*) o unidad máxima de transferencia, que es el tamaño máximo de segmento que puede viajar a través de una red determinada, esto quiere decir que la MTU puede variar según la configuración de la red. La capa de transporte asigna una identificación de punto de acceso a servicio (*SAP Service Access Point*) o número de puerto (como lo nombra TCP/IP). La ID SAP indica qué aplicación o proceso se ejecuta. Es por ello que puede haber diferentes aplicaciones ejecutándose simultáneamente en una misma estación, pues cada aplicación corresponde a un número de puerto. Un ejemplo de aplicaciones podría ser que una estación esté navegando en Internet por medio de la aplicación http que tiene como número de puerto 80, y simultáneamente esté descargando archivos de un servidor ftp (*File Transfer Protocol* o protocolo de transferencia de archivos) el cual utiliza el puerto 21.

Aunque como se mencionó antes, la capa de enlace de datos y de red puede hacer la comprobación de errores, ésta es una responsabilidad propia de la capa de transporte. Existen dos tipos de entrega para la capa de transporte, la primera es la entrega fiable y significa que detecta los errores y los corrige, a este tipo de entrega también se le denomina entrega dedicada a conexión. La segunda es la entrega no fiable en la cual existen errores en la transmisión pero no se verifican pues se requiere una transmisión más rápida y menos consumo de ancho de banda, a este tipo de entrega también se le denomina no orientada a conexión y se prefiere cuando el número de mensajes es alto.

La quinta capa es la capa de sesión, esta capa es la encargada de proporcionar los mecanismos para el control del diálogo entre las distintas aplicaciones entre estaciones. Esta capa permite que los nodos se comuniquen de manera organizada y se puede regir por tres fases. La primera es el establecimiento de conexión en la cual las estaciones negocian las reglas de



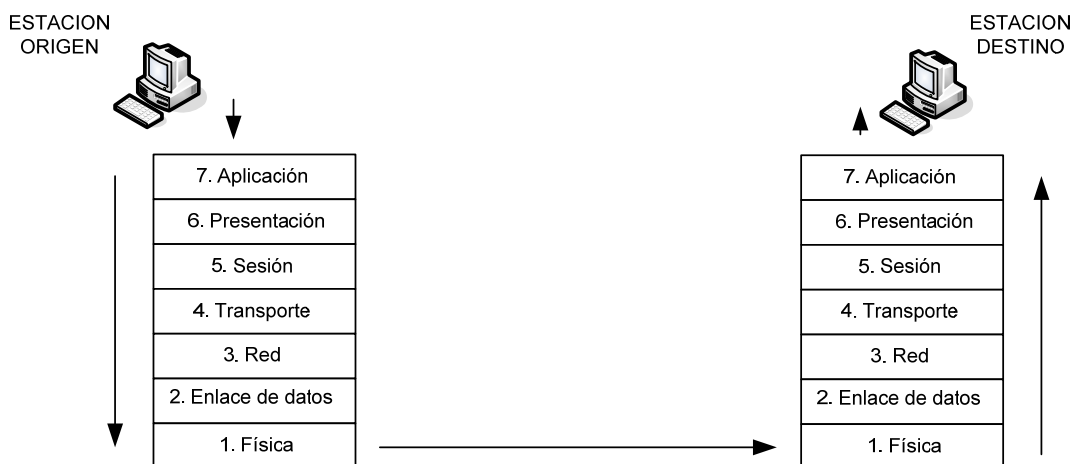
comunicación incluyendo los protocolos utilizados. La segunda fase es la transferencia de datos donde las estaciones inician el diálogo, y la tercera fase es la liberación de la conexión. Como se mencionó, la capa de sesión es la encargada del control del diálogo, esto se puede realizar simultáneamente en los dos sentidos (full duplex) o alternadamente en los dos sentidos (half duplex). A partir de esta capa y hasta llegar a la capa de aplicación el pdu se le conoce como datos.

La capa de presentación es la responsable de presentar los datos a la capa de aplicación, esto quiere decir que es la encargada de la sintaxis y la semántica de la información transmitida. Otras funciones que corresponden a esta capa son la encriptación y compresión de los datos, que es parte de la seguridad que se puede incluir en la transmisión de los datos. Un ejemplo del trabajo que realiza esta capa podría ser cuando una computadora IBM, que utiliza codificación EBCDIC, trata de comunicarse con una PC la cual utiliza codificación ASCII, entonces la capa de presentación se encarga de traducir de uno a otro tipo de codificación para que se puedan entender las estaciones. Esta capa se podría comparar con una persona traductora la cual nos traduce de una lengua extranjera a nuestra lengua para que podamos entender lo que nos están diciendo.

La última capa del modelo OSI es la capa de aplicación, que es la capa con la cual el usuario tiene contacto. Proporciona los servicios utilizados por las aplicaciones para que los usuarios se comuniquen a través de la red. Algunos ejemplos de las aplicaciones podrían ser el transporte de correo electrónico, el acceso a archivos remotos, la ejecución de tareas remotas, las transferencias de ficheros y la administración de la red entre otros. Como se mencionó para cada aplicación existe un número de puerto relacionado o API (como se le denomina en UNIX) o socket (como se le denomina en Windows).

Cuando una estación origen desea enviar un mensaje a una estación destino, el mensaje debe comenzar en la capa de aplicación de la estación origen y debe de terminar en la capa física de esa misma estación, luego viaja a través del medio físico y llega a la capa física de la estación destino, sube por todas las capas hasta llegar a la capa de aplicación de la estación destino, con lo cual la trayectoria del mensaje se ha completado y la comunicación entre las dos estaciones se ha llevado a cabo. Esto se ilustra en la figura 24.

**Figura 24. Proceso de comunicación entre dos estaciones**



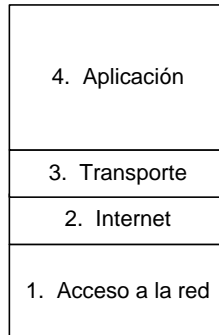
## 2.2 Modelo TCP/IP

El modelo TCP/IP fue utilizado por primera vez en la red que desarrolló la ARPA (*Advance Resource Project Agency* o agencia de proyectos de investigación avanzada) y que se le denominó ARPANET. La ARPANET surgió como necesidad ante los problemas que podían suscitar durante la Guerra Fría en la década de 1950, cuando hasta entonces todas las comunicaciones militares usaban la red telefónica pública que se consideraba vulnerable pues

todos los teléfonos se conectaban a una oficina de conmutación telefónica y éstas a su vez se conectaban a oficinas de conmutación interurbanas, entonces con la destrucción de algunas de las oficinas interurbanas se podía fragmentar el sistema en muchas islas incomunicadas. Entonces la DOD (*Department of Defense* o departamento de defensa) financió los estudios de un nuevo sistema de comunicación que no fuera tan vulnerable. Durante la investigación surgieron varios modelos que se fueron modificando y mejorando hasta la culminación con la invención del modelo TCP/IP en el año de 1974 por Cerf y Kahn. TCP/IP está diseñado de manera específica para manejar comunicación por interredes. Durante los años ochenta se creía que OSI llegaría a imponerse frente a diferentes arquitecturas que existían en esa época y frente a TCP/IP, pero en los años noventa TCP/IP se logró posicionar como la arquitectura comercial dominante, y esto se debió a que TCP/IP se comenzó a utilizar de una forma más generalizada antes que la normalización ISO, dado a que la DOD necesitaba un conjunto de protocolos para antes de los años ochenta. Debido a que en esa época DOD era el consumidor más grande de software en el mundo, y ellos utilizaron TCP/IP, el mercado consecuentemente comenzó a desarrollar productos basados en TCP/IP para satisfacer dicha demanda y fue así como TCP/IP llegó a ser el principal modelo o conjunto de protocolos para la comunicación entre estaciones y redes.

El modelo o conjunto de protocolos TCP/IP consta de 4 capas las cuales se ilustran en la figura 25.

**Figura 25. Capas del modelo TCP/IP**



La primera capa es la capa de acceso a la red o también denominada host a red. Esta capa se encarga del intercambio de datos entre una estación y la red y entre los dispositivos de la misma red. En esta capa se incluyen los detalles de la tecnología LAN y WAN que utiliza la red. Esta capa define los procedimientos para realizar la interfaz con el hardware de la red y para poder obtener acceso al medio de transmisión físico. Como su nombre lo indica en esta capa se definen todos los procedimientos para que una estación pueda acceder a la red, además se definen las direcciones físicas o direcciones MAC que serán utilizadas por la capa Internet para asociarla a una dirección lógica o dirección IP. La capa física y de enlace de datos del modelo OSI son comprendidas en la capa de acceso a la red y todas las características que se explicaron anteriormente para estas dos capas del modelo OSI describen también a esta capa.

La segunda capa del modelo TCP/IP es la capa de Internet, esta capa al igual que la capa de red del modelo OSI, su propósito es escoger la mejor ruta para poder encaminar un paquete a través de todas las redes que estén en el camino desde la estación origen hasta la estación destino. Además esta capa provee el direccionamiento lógico o dirección IP que se asigna a cada estación

la cual es utilizada por los protocolos de capas superiores para poder identificar a que estación destino enviarán los datos y a que red pertenecen. El protocolo de resolución de direcciones (ARP) permite que el protocolo enrutado IP identifique la dirección física que corresponde a una dirección lógica IP. Los protocolos principales que operan en esta capa son el protocolo enrutado IP (*Internet Protocol*), ARP, ICMP (*Internet Control Message Protocol* o protocolo de Internet de control de mensaje) que es el responsable de proveer diagnósticos de funciones y reportar errores en la entrega, pero no corrige errores, e IGMP (*Internet Group Management Protocol* o protocolo de Internet de manejo de grupo) que es el responsable del manejo de grupo de multicast o multitransmisión.

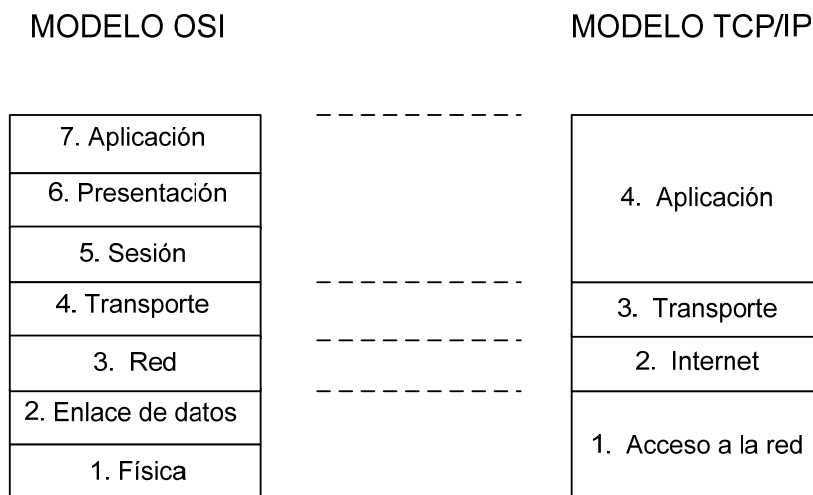
La capa 3 del modelo TCP/IP es la capa de transporte, tiene las mismas funciones que la capa de transporte del modelo OSI anteriormente explicada. A esta capa también se le conoce como capa de host a host. La capa de transporte es la responsable de proveer las herramientas para que los paquetes sean transmitidos desde una estación origen a una estación destino. En esta capa los paquetes de capa 2 se encapsulan y se les agrega una cabecera para formar lo que es un segmento. La capa de transporte lleva un control de cada segmento transmitido y dependiendo de que protocolo se utilice puede corregir los errores y retransmitir segmentos que no llegaron o llegaron corrompidos a su destino. Además esta capa ofrece el control de flujo, con lo cual el host destino le dice al host origen que envíe más lento o más rápido los segmentos. Los protocolos que trabajan en esta capa son el protocolo de control de transmisión (TCP) y el protocolo de datagrama de usuario (UDP).

La última capa del modelo TCP/IP es la capa de aplicación. En esta capa al igual que en el modelo OSI, se encuentran las aplicaciones que no son más que las interfaces para acceder a los servicios de las demás capas inferiores.

Existen muchas aplicaciones hoy en día, y se continúan desarrollando nuevas. A cada aplicación se le asigna un socket o un número de puerto en particular, para que una estación pueda estar ejecutando diferentes aplicaciones. Las aplicaciones más conocidas son las tipo http (*Hyper Terminal Transfer Protocol*), las ftp (*File Transfer Protocol*), las de correo electrónico, etc. Cada uno de estos puertos dependiendo del protocolo de capa de transporte utilizado, son especificados en el RFC (*Request For Comments*) publicados por la IETF, para TCP es el RFC793 y para UDP es el RFC768.

En la figura 26 se ilustra una comparación entre el modelo OSI y el modelo TCP/IP, en la cual se puede observar que capas del modelo OSI son abarcadas por el modelo TCP/IP.

**Figura 26. Comparación entre OSI y TCP/IP**

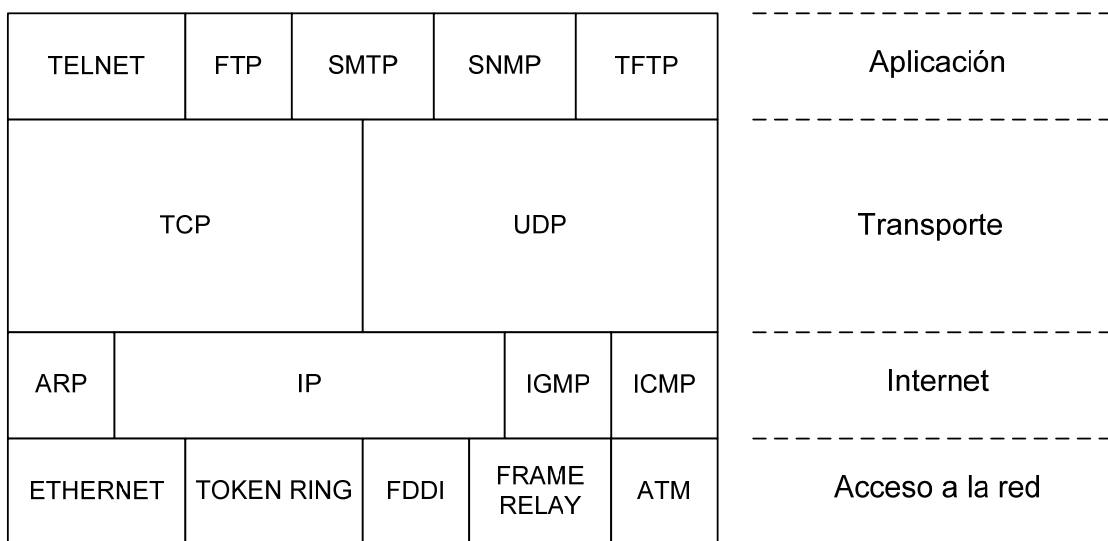


### 2.3 Principales protocolos del conjunto TCP/IP

El modelo TCP/IP es un conjunto de varios protocolos que trabajan en diferentes capas, de todos estos protocolos los que más sobresalen y que más se utilizan son el IP de capa 3 OSI y el protocolo orientado a conexión TCP, de aquí el nombre TCP/IP. También podría existir la combinación UDP/IP o TCP/IPX por ejemplo.

En cada capa del modelo TCP/IP trabajan ciertos protocolos y aplicaciones, algunos de ellos se ilustran en la figura 27.

**Figura 27. Arquitectura de protocolos de TCP/IP.**



Existe un grupo de protocolos del conjunto TCP/IP que se consideran el corazón o centro de TCP/IP y que se les considera como los principales protocolos, estos son IP, ARP, ICMP, IGMP, TCP y UDP. Todas las demás aplicaciones y protocolos de TCP/IP dependen de este centro o corazón.

El ARP o *Address Resolution Protocol*, es un protocolo que se utiliza para obtener la dirección MAC de una dirección IP en particular. ARP se utiliza en redes de accesos compartidos y redes basadas en broadcast tal como ethernet y token ring. El protocolo ARP está definido en el RFC 826. Para una estación origen obtener una dirección MAC, éste envía un marco de solicitud ARP en el cual está contenida la dirección IP y MAC del origen, la dirección IP del destino y también un mensaje de broadcast con el formato FF:FF:FF:FF:FF:FF:FF:FF en hexadecimal. Este mensaje es recibido por todas las estaciones de la red y comparan la dirección IP de destino con la suya. Si coincidieran las IP, entonces la estación destino crea un marco de respuesta ARP que contiene su dirección MAC e IP y lo devuelve a la estación que ha emitido la solicitud, con ello el protocolo ARP recibe la información y se lo entrega al protocolo IP. ARP tiene en una tabla caché las direcciones MAC que se hayan recibido recientemente y con ello reduce el número de solicitudes de direcciones. Estas tablas son consultadas antes de difundir solicitudes ARP, y tienen un período de vida limitado que está determinado por el administrador del sistema. Cada estación dentro de una LAN responde a la petición broadcast de ARP, en el caso en que a ninguna estación correspondiera la IP destino, entonces el router es el encargado de verificar si en sus tablas ARP aparece la dirección IP que se está buscando, y si la encuentra entonces envía de vuelta el par IP-MAC por la interface por la cual fue solicitado.

Adicionalmente ARP utiliza como complemento el protocolo RARP (*Reverse Address Resolution Protocol*) que permite que se pueda determinar una dirección IP por medio de su dirección MAC. El protocolo RARP es muy utilizado por aquellos dispositivos que no tienen un disco y deben arrancar desde la red, cuando arrancan, generan una solicitud RARP para determinar su IP, esta dirección es dada por un servidor que generalmente es un encaminador. El formato de la petición RARP está constituido por las



direcciones MAC origen y destino; así como también de la dirección IP destino y el mensaje de broadcast que utiliza ARP. Como se podrá comprender el proceso de obtención de la información es parecida para los dos protocolos. Ambos protocolos operan en la capa de Internet.

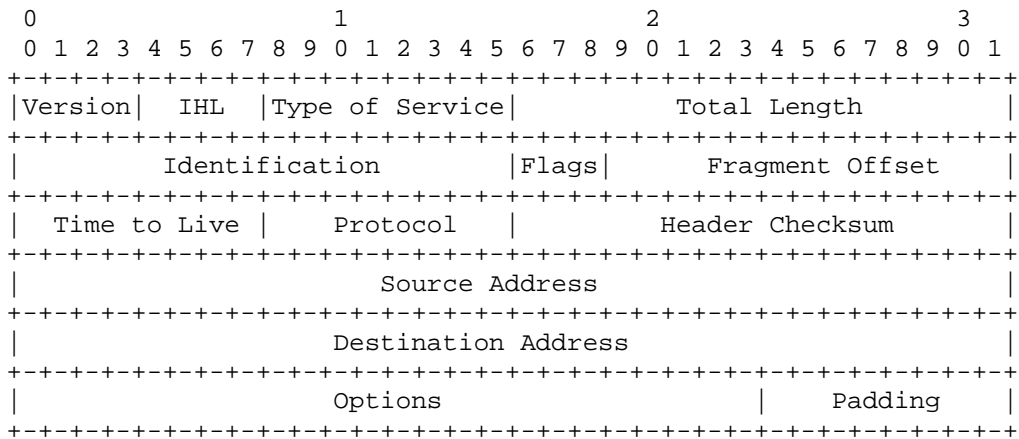
Los protocolos IP, IGMP, ICMP, TCP y UDP que forman parte de este centro de protocolos de TCP/IP serán tratados más adelante.

## **2.4 Características de IP versión 4**

IP o protocolo de Internet es un protocolo no orientado a conexión, poco confiable que su principal función es el direccionamiento y crear paquetes que puedan ser encaminados entre estaciones. No orientado a conexión significa que la conexión no es establecida antes de comenzar a transmitir datos. Poco confiable se refiere a que la entrega de los paquetes no es garantizada, estos trabajos son responsabilidad de las capas superiores y por ello IP no lo ejecuta. La versión de este protocolo que se está utilizando actualmente es la versión 4, de ahí que su nombre resumido sea IPv4. Esta versión es especificada en el RFC 791 publicada en Septiembre de 1981 y que está basado en 6 ediciones anteriores, esto quiere decir que este RFC es una actualización de 6 anteriores.

El formato de la cabecera de un paquete IP o datagrama versión 4 se ilustra en la figura 28, donde se puede observar cada uno de los campos que conforma dicha cabecera.

**Figura 28. Formato de la cabecera de un paquete IP versión 4**



Fuente: RFC 791, página 10.

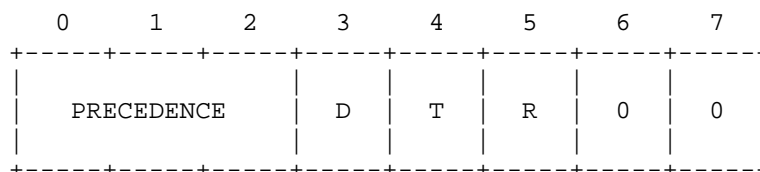
El primer campo que presenta esta cabecera es el campo de versión e indica el formato o versión que la cabecera está utilizando, este campo está compuesto por 4 bits. En la actualidad este campo indica la versión 4 en la mayoría de redes. Las redes que ya están utilizando IP versión 6, deben de tener en este campo versión 6.

El campo IHL (*Internet Header Length*) o longitud de la cabecera de interred, indica la longitud de la cabecera en palabras de 32 bits. El tamaño mínimo admitido es de 5 palabras, que según la figura 28 llegaría hasta la dirección destino. Este campo también está compuesto por 4 bits.

El campo tipo de servicio, es un campo de 8 bits. Este campo indica la calidad del servicio deseado. Estos parámetros se utilizan para guiar la selección de los parámetros del actual servicio o tecnología que se está utilizando cuando se va a transmitir el datagrama a través de una red en particular. Es decir el efecto de los valores de estos campos depende de la tecnología de la red utilizada. El TOS (*Type of service*) se utiliza para manejar

cierta prioridad en el tráfico que se está transmitiendo, pues por ejemplo para la transmisión de voz digital es más importante la velocidad y no la entrega precisa, caso contrario sucede con la transferencia de archivos en donde es más importante una entrega sin errores que una entrega rápida. Este campo es uno de los campos que ha cambiado levemente su significado en el transcurrir de los años. En sus inicios este campo usaba 3 bits para un sub campo denominado precedencia ó prioridad, además usaba otros 3 bits que se les denominaba banderas, que eran D (*Delay* o retardo), T (*Troughput* o velocidad real de transporte) y R (*Reliability* o confiabilidad), los últimos dos bits no se utilizaban y aún hoy en día se tienen reservados para un futuro uso, es por ello que se decía que este campo constaba de 6 bits. El formato de este campo se presenta en la figura 29.

**Figura 29. Formato del campo TOS**



Fuente: RFC 791, página 12.

El campo precedencia es una prioridad, de 0 que es lo normal, a 7 que es el máximo. El bit D si toma valor de 0 es porque se necesita un retardo normal, si toma valor de 1 necesita un retardo bajo. El bit T con valor de 0 es una velocidad real de transporte normal, con valor de 1 es una velocidad alta. El bit R con valor de 0 es una confiabilidad normal, con valor de 1 se tiene una confiabilidad alta. En la práctica, éste campo no es muy utilizado por los routers, pues muchas veces éstos parámetros son establecidos por protocolos de capas superiores.

El campo longitud, es un campo compuesto por 16 bits, que nos indica la longitud total del datagrama, medido en octetos (8 bits) o bytes, que incluye la cabecera y los datos. Este campo es necesario pues indica donde termina un datagrama y con ello se puede determinar cuando comienza otro datagrama. Dado que está compuesto de 16 bits, la longitud máxima es de  $2^{16} - 1 = 65,535$  bytes. Esta longitud ya no es tolerable para redes gigabit ethernet, las cuales requieren datagramas más grandes. Es normado que las estaciones envíen únicamente datagramas de longitud de por lo menos 576 bytes.

El campo identificación es un campo de 16 bits, el cual es necesario para que la estación determine a qué datagrama pertenece un fragmento recién recibido. Esta identificación es asignada por el emisor para ayudar en el ensamblaje de los fragmentos del datagrama, existe un único identificador para todos los fragmentos que corresponden a un mismo datagrama.

El siguiente es el campo de Flags o banderas, el cual está compuesto por 3 bits que también se les denomina indicadores de control. El bit más significativo o bit 0, está reservado y su valor debe ser 0. El bit 1 ó bit DF (*Don't fragment* o no fragmentar), puede tomar los valor de 0 el cual indica a los enrutadores que el datagrama puede fragmentarse y el valor de 1 cuando no se puede fragmentar. El bit menos significativo (bit 2) o bit MF (*More Fragments* o más fragmentos), éste es un indicador que tienen todos los fragmentos excepto el último que conforma el datagrama, pues indica cuando han llegado todos los fragmentos al destino.

El campo Fragment offset o desplazamiento de fragmento, es un campo de 13 bits, el cual indica en qué parte del datagrama actual va un fragmento en específico. Todos los fragmentos exceptuando el último deben tener un

múltiplo de 8 bytes, que es la unidad de fragmentos elemental. El máximo de fragmentos por datagrama es de  $2^{13} = 8192$ .

El campo tiempo de vida o *time to live*, es un campo de 8 bits que indica el tiempo máximo que puede existir un datagrama en una red. Este es prácticamente un contador que se va decrementando cada vez que un datagrama pasa por un encaminador. La unidad de medida son segundos, permitiendo una vida máxima de 255 segundos. En la práctica este contador simplemente cuenta los saltos o enrutadores que va pasando. Cuando el contador tiene un valor de cero, el paquete se destruye y se envía de regreso un mensaje ICMP que se verá más adelante. Este contador garantiza que los datagramas no entregados sean eliminados y no se queden vagando eternamente en la red.

El campo protocolo, es un campo compuesto de 8 bits que indica el protocolo de las capas superiores al que debe entregarse el paquete. El RFC 1700 contiene los números asignados a muchos protocolos.

El campo checksum header o suma de verificación de cabecera, es un campo compuesto de 16 bits, el cual su función es hacer una suma de verificación para la detección de errores generados por palabras de memoria erróneas en un encaminador. Esta verificación la hace únicamente para la cabecera y se debe realizar en cada salto o encaminador que pase, pues al menos uno de los campos del datagrama cambia (tiempo de vida) cuando da un salto y debe volver a hacer la suma de verificación. El algoritmo utilizado suma todas las series de 16 bits conforme van llegando, para ello utiliza la aritmética de complemento a uno, y luego obtiene el complemento a uno del resultado. La suma de verificación se establece con un valor de 0 para efectos del algoritmo.

Los campos *source* y *destination address* o direcciones origen y destino respectivamente, son campos compuestos cada uno por 32 bits, pues en la versión 4 de IP se manejan direcciones de 32 bits agrupados en 4 octetos, esto se detallará más adelante. Estos dos campos indican la dirección IP del host origen y la dirección IP del host destino.

El último campo en este datagrama de IP versión 4, es el campo de opciones, este campo como su nombre lo indica puede o no utilizarse. Este campo cuando se usa en IPv4 su función muchas veces es para hacer experimentos, probar nuevas ideas y para evitar la asignación de bits de encabezado a información pocas veces necesaria. Este campo es de longitud variable. Cada opción comienza con un código de 1 octeto. Algunas opciones van seguidas de un campo de longitud y luego de uno o más octetos de datos. Este campo es utilizado para completar múltiplos de 32 bits o sea 4 octetos.

En la tabla III se puede observar los distintos tipos de opciones que existen para IPv4.

**Tabla III. Tipos de opciones del datagrama IPv4**

No.	OPCION	DESCRIPCION
0	Fin de la lista de opciones	Ocupa 1 byte, no tiene longitud de octeto.
1	No operación	Ocupa 1 byte, no tiene longitud de octeto.
2	Seguridad	Utilizada para brindar seguridad, especifica que tan secreto es el datagrama.
3	Enrutamiento libre desde el origen	Da una lista de los enrutadores que no deben evitarse.
4	Marca de tiempo	Hace que cada enrutador agregue su dirección y su marca de tiempo.

7	Registrar ruta	Hace que cada enrutador agregue su dirección IP.
8	Identificador de línea	Lleva la identificación de la línea.
9	Enrutamiento estricto desde el origen	Indica la ruta completa a seguir.

Algunas de estas opciones son bien importantes como la de seguridad, la de enrutamiento estricto desde el origen, la de enrutamiento libre desde el origen, la de registrar ruta y la opción marca de tiempo.

La opción seguridad se usa para especificar que el datagrama se encamine por una cierta ruta, la cual se considera una ruta segura, esto podría servirle a la milicia, si ellos no quisieran que su información pase por cierto país por ejemplo. El formato para esta opción seguridad se ilustra en la figura 30.

**Figura 30. Formato de la opción seguridad en IPv4**

```

+-----+-----+---//---+---//---+---//---+---//---+
|10000010|00001011|SSS SSS|CCC CCC|HHH HHH| TCC  |
+-----+-----+---//---+---//---+---//---+---//---+
Type=130 Length=11

```

Fuente: RFC 791, página 17.

El campo S, es un campo de 16 bits que especifica uno de los 16 niveles de seguridad, ocho de los cuales están reservados para futuros usos. El campo C, es un campo de 16 bits, es un campo que si todos sus bits tienen valor igual a cero, entonces la información no está compartida, otros valores para este campo pueden ser obtenidos de la Agencia Inteligente de Defensa. El campo H, es un campo de 16 bits que se encarga de las restricciones. Dichas restricciones están definidas en el DIAM 65-19 (Manual de la agencia inteligente de defensa). El campo TCC o código de control de transmisión (*Transmision*

*Control Code*), es un campo de 24 bits que define comunidades de interés controladas entre suscriptores.

La opción de enrutamiento estricto desde el origen, brinda la ruta completa desde el origen hasta el destino. Es necesario que el datagrama siga dicha ruta exacta. Esto es utilizado cuando en un enrutador se pierde la tabla de enrutamiento y es necesario enviar datagramas de emergencia con la ruta especificada. Esto quiere decir que el paquete debe seguir exactamente cada uno de los saltos que se especifican en dicha ruta, no puede tomar una ruta alterna, aunque dicha ruta alterna sea mejor.

La opción de enrutamiento libre desde el origen, requiere que el datagrama pase por los enrutadores indicados en la lista, y en el orden especificado, pero puede pasar por otros enrutadores en dicho trayecto.

La opción de registrar ruta, indica a los enrutadores que registren su dirección IP al campo de opción. Con esto los administradores de las redes pueden determinar fallas en los algoritmos de enrutamiento.

La opción de marca de tiempo, indica a los enrutadores que registren una marca de tiempo de 32 bits. La unidad de medida de esta opción está en milisegundos desde la media noche UT (*Universal Time*). Esta opción también se utiliza para detectar fallas en los algoritmos de enrutamiento.

#### **2.4.1 ICMPv4**

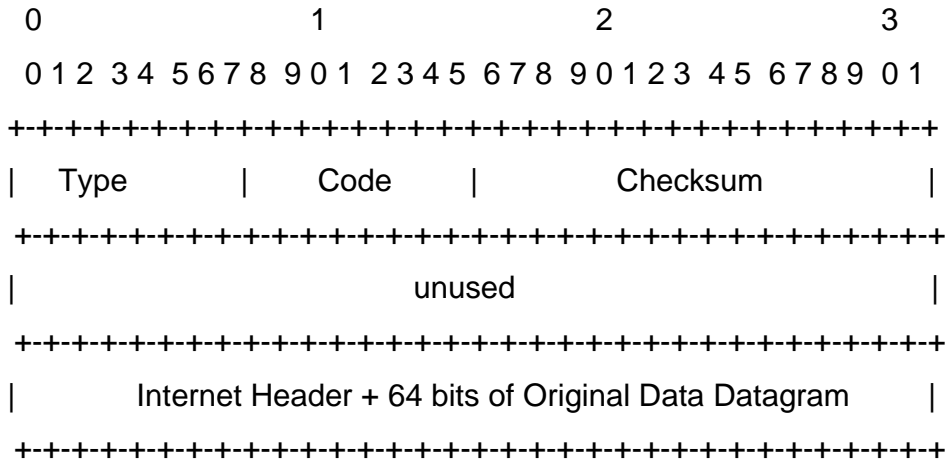
El protocolo ICMP o protocolo de mensajes de control de Internet es un protocolo que viene a complementar a IP dado que IP es un protocolo de entrega de mayor esfuerzo y no tiene el mecanismo para poder detectar errores



ni para corregirlos. ICMP es el encargado de detectar y notificar a las fuentes, de los errores que se producen en la entrega de datagramas, pero no puede corregirlos como se mencionó anteriormente. La confiabilidad y la corrección de errores son proporcionadas por los protocolos de capas superiores. Estos mensajes se envían por ejemplo cuando una estación no puede alcanzar el destino o cuando el Gateway o puerta de enlace no tiene la suficiente capacidad en el buffer, entre otros. Los mensajes ICMP son notificados únicamente al dispositivo emisor, no se envía ninguna información sobre los cambios de la red a ningún encaminador que esté en la trayectoria que haya tomado el paquete hacia el destino.

Los mensajes de ICMP se encapsulan en datagramas, del mismo modo en que se entrega cualquier otro paquete mediante el uso de IP. Debido a que estos mensajes se transmiten de la misma manera que cualquier otro paquete, están sujetos a la misma falla de entrega, esto crea una situación como la que se trató anteriormente, en la que un informe de error puede generar más informes de error, lo cual provocaría una congestión en la red debido a la cantidad de mensajes de notificación de error. Es por ello que ICMP no envía mensajes de error cuando no se logra entregar otro paquete ICMP. La figura 31 muestra el formato de un mensaje ICMP general, el cual es presentado en el RFC 792.

**Figura 31. Formato de un mensaje ICMPv4**



Fuente: RFC 792, página 3

El campo Tipo, es el primer octeto y este octeto se utiliza para identificar uno de los varios tipos de mensajes ICMP que existen, cada uno de los tipos de mensajes se presenta en la tabla IV.

**Tabla IV. Tipos de mensajes ICMPv4**

TIPO	ICMPv4 mensajes
0	Respuesta de eco
3	Destino inalcanzable
4	Disminución de velocidad en origen (source quench)
5	Redireccionar / cambiar dirección
8	Petición de eco
9	Publicación de router
10	Selección del router
11	Tiempo superado o Time exceeded
12	Problema de parámetros

13	Petición de marca horaria
14	Respuesta de marca horaria
15	Petición de información
16	Respuesta de información
17	Petición de máscara de dirección
18	Respuesta de máscara de dirección

El segundo campo es el de código, éste consta de 8 bits y se utiliza para especificar parámetros del mensaje. Contiene información relacionada con el tipo de mensaje. El campo *Checksum* o suma de comprobación utiliza el mismo algoritmo de suma de comprobación que en IP. El campo *Unused* o sin usar, es un campo reservado para futuras extensiones y debe tener un valor igual a 0.

En el último campo aparece la cabecera IP básica y como complemento 64 bits del campo de datos del datagrama original, esto se incluye en aquellos mensajes que se refieren a datagramas. La razón de incluir estos 64 bits es para que el computador pueda determinar qué protocolo de capa superior están implicados en el mensaje.

Los mensajes de petición de eco y respuesta de eco proporcionan un mecanismo para comprobar la posibilidad que dos estaciones puedan comunicarse. Este tipo de mensajes es el que se utiliza cuando se ejecuta el comando ping, el host A emite un mensaje de petición de eco hacia el host B, si el paquete llega al destino, éste le responde con un paquete de respuesta de eco. El formato de los mensajes de eco se muestra en la figura 32.

**Figura 32. Formato de un mensaje ICMP de eco**

TIPO (8)	CODIGO (8)	SUMA DE COMPROBACION (16)
IDENTIFICADOR (16)		NUMERO DE SECUENCIA (16)
DATOS OPCIONALES (32)		

El identificador se puede utilizar como un punto de acceso al servicio para identificar una sesión en particular, y el número de secuencia se puede incrementar en cada petición de eco enviada.

Otro mensaje que aparece cuando se envía una petición de eco es el mensaje de destino inalcanzable o *destination unreachable*, que se obtiene como resultado de un paquete que no llega a su destino. Por ejemplo, si una estación A envía una petición de eco a la estación B, A y B están comunicadas por medio de un encaminador, si el encaminador no tiene la ruta desde A para encontrar B, entonces cuando se haga la petición dicho encaminador le responderá a la estación A con un mensaje ICMP de destino inalcanzable. El formato de este tipo de mensaje se presenta en la figura 33.

**Figura 33. Formato de un mensaje ICMP de destino inalcanzable**

TIPO (8)	CODIGO (8)	SUMA DE COMPROBACION (16)
SIN USAR (32)		
CABECERA IP + 64 BITS DEL DATAGRAMA ORIGINAL		

Para este tipo de mensajes en la tabla V se muestran los diferentes códigos posibles.

**Tabla V. Tipos de códigos ICMPv4 de destino inalcanzable**

CODIGO	DESCRIPCION
0	Red inalcanzable
1	Host inalcanzable
2	Protocolo inalcanzable
3	Puerto inalcanzable
4	Fragmentación necesaria
5	Falla de ruta origen
6	Red de destino desconocida
7	Host de destino desconocido
8	Host de origen aislado
9	Comunicación con red destino prohibida por la administración
10	Comunicación con host destino prohibida por la administración
11	Red inalcanzable por tipo de servicio
12	Host inalcanzable para el tipo de servicio

Para cada tipo de mensaje ICMP existen diferentes tipos de códigos.

Otro mensaje muy común es el mensaje de tiempo excedido, que se obtiene del resultado de un paquete que se ha vencido el TTL (tiempo de vida), esto quiere decir que el paquete ha viajado por la red y en cada paso por un encaminador ha disminuido su TTL hasta llegar a un valor cero, entonces el encaminador en el que se ha quedado envía un mensaje de tiempo de vida excedido. El formato de dicho mensaje es igual al de destino inalcanzable presentado en la figura 33.

### 2.4.2 IGMPv4

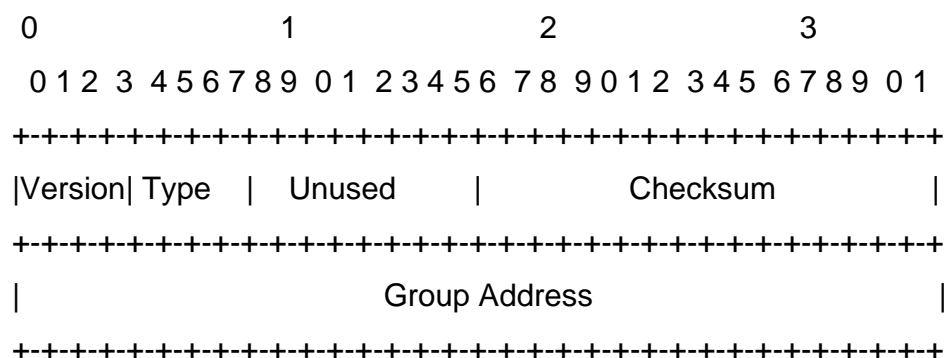
IGMP de sus siglas en inglés, *Internet Group Management Protocol* o protocolo de gestión de grupos de Internet, es un protocolo que gestiona las estaciones que son miembros de un grupo multicast (multidifusión). Un grupo IP multicast también es conocido como grupo de estaciones pues está formado por varias estaciones o hosts que se encuentran escuchando el tráfico IP que está destinado específicamente a ese grupo, es decir que las estaciones que no pertenezcan a ese grupo, no podrán escuchar dicho tráfico. El tráfico IP multicast está destinado a una sola dirección IP pero es procesado por múltiples estaciones. Los miembros de un grupo multicast pueden unirse o desintegrarse del grupo dinámicamente en cualquier momento. El tamaño del grupo puede ser variable y los hosts pueden pertenecer a uno o varios grupos a la vez. Una estación que no pertenezca a un grupo multicast puede enviar tráfico dirigido a ese grupo sin ninguna limitante. Los grupos multidifusión pueden ser permanentes o dinámicos. Los permanentes son aquellos grupos que tienen asignado una IP de manera estática y que inclusive pueden no llegar a tener integrantes, el grupo todavía sigue existiendo. Los dinámicos son aquellos grupos que poseen una IP de manera dinámica y el grupo deja de existir cuando ya no tiene miembros.

Una estación puede soportar multidifusión IP en tres niveles, el primer nivel es el nivel 0 en el cual la estación no puede enviar ni recibir tráfico IP multidifusión. El segundo nivel es el nivel 1 en el cual la estación no puede recibir pero si enviar tráfico multidifusión. El último nivel que es el nivel 2, en este nivel la estación puede enviar y recibir tráfico multidifusión IP. El nivel 2 requiere que se implemente IGMP. Los mensajes IGMP pueden tomar dos formas, la primera es cuando una estación se une a un grupo, entonces esta estación envía un mensaje IGMP reportándose con todas las demás estaciones

del grupo y esto lo hace por medio de la dirección 224.0.0.1, esta dirección está asignada para direccionar a todas las estaciones de un grupo multicast. La segunda forma es cuando un encaminador envía un mensaje a todas las estaciones de un grupo para asegurarse que hay algún miembro o miembros en dicho grupo, si después de varias consultas que ha hecho el encaminador ninguna estación le contesta, el encaminador asume que no existe ninguna estación en dicho grupo.

IGMP es el protocolo encargado de registrar la información de las estaciones de un grupo multicast. Este protocolo está definido en el RFC 1112 y es utilizado tanto por los dispositivos de encaminamiento como por las estaciones para intercambiar información de grupo de multicast sobre una LAN. Al igual que ICMP, IGMP es una parte integral del protocolo IP. Los mensajes IGMP son encapsulados en datagramas IP y el formato que tienen dichos mensajes se presenta en la figura 34.

**Figura 34. Formato de un mensaje IGMP de destino inalcanzable**



Fuente: RFC 1112, página 10

El primer campo de este datagrama es el campo de versión, el cual está conformado por 4 bits, la versión antigua es la versión 0 y la que se trata en el RFC 1112 es la versión 1.

El segundo campo es el campo tipo, este campo indica qué tipo de mensaje IGMP es, como se mencionó anteriormente puede ser el mensaje de reporte de pertenencia a un grupo o puede ser el mensaje de requisición de pertenencia a un grupo. Este campo también es de 4 bits.

El campo sin usar o *unused* es un campo conformado por 8 bits y debe tener un valor de cero. El campo de *checksum* o suma de comprobación, es un campo de 16 bits que utiliza el complemento de uno de los 8 bytes que conforman el mensaje IGMP.

El último campo es el campo de dirección de grupo o *group address*, el cual está conformado por 32 bits. Este campo es puesto en cero cuando el tipo de mensaje es un mensaje de requisición de pertenencia a un grupo y cuando es un mensaje de reporte de pertenencia a un grupo, contiene la dirección IP del grupo que se está reportando.

## **2.5 Direccionamiento IP en versión 4**

El protocolo IP es un protocolo enrutado el cual ofrece direccionamiento, fragmentación y reensamblaje de datagramas y entrega de datagramas a través de la interred. Una dirección IP en versión 4 está compuesto por 4 campos de 8 bits y cada campo es separado por un punto “.”. El direccionamiento IP o direccionamiento de capa de internet es necesario para poder identificar a una interfaz de un dispositivo con una única dirección como miembro de una red en específico, pues la identificación de un nodo en una interred requiere el uso de



la red a la que pertenece y la identificación del nodo en dicha red. La dirección IP no es igual que la dirección MAC, pues la dirección IP está en la capa 3 del modelo OSI y la dirección MAC en la capa 2. La dirección MAC es una dirección física fija que es asignada por el fabricante de la interfaz, mientras que la dirección IP es una dirección lógica que puede variar para cada interfaz. La dirección IP es la dirección utilizada por los protocolos de capas superiores y ésta puede soportar cambios de hardware, pues si se cambiara la tarjeta adaptadora de red de un host, su dirección IP puede configurarse para que sea la misma y no varíe.

### **2.5.1 Formato de una dirección IPv4**

Una dirección IP en versión 4 es un conjunto de unos y ceros cuya longitud es de 32 bits, lo cual da  $2^{32} = 4,294,967,296$  direcciones IP posibles. Como se mencionó anteriormente cada octeto está separado por un punto, el primer octeto es el de la izquierda y el cuarto octeto es el de la derecha. El formato que se maneja es en base decimal para que su uso sea más sencillo y comprensible, esto se muestra a continuación:

Dirección IP en base 2 (Formato binario):

10101100.00010000.00000011.01010101

Dirección IP en base 10 (Formato decimal):

172.16.3.85

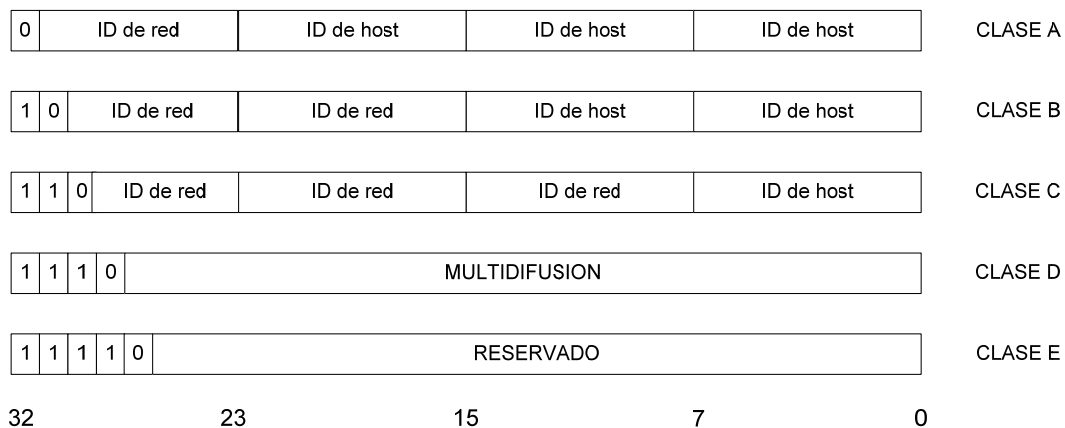
En base decimal cada octeto va de un valor 0 a un valor 255 e igual están separadas por un punto decimal, este formato es denominado notación decimal punteada. En base 2 el bit menos significativo es el bit más a la derecha y el más significativo es el que está más a la izquierda.

Las direcciones IP constan de dos campos, los cuales son, el campo de identificador de red o netid, y el campo identificador de host o hostid. El campo identificador de red es el encargado de identificar a que red pertenece la estación, y el campo identificador de host es el identificador asignado único para cada interfaz, servidor, encaminador o cualquier otra estación en específico.

### 2.5.2 Clases de direcciones en IPv4

En los inicios, IP en su versión 4 fue definido originalmente con cinco clases de direcciones para acomodar redes de varios tipos de tamaño, pues se observó la necesidad de poder tener redes de distintos tamaños. La figura 35 muestra las cinco clases de direcciones IP.

**Figura 35. Clases de direcciones IPv4**



En las direcciones clase A, el primer octeto es identificador de red y los tres restantes son de host, estas direcciones comienzan con un valor igual a cero en el bit más significativo. El rango de esta clase es de 0 a 127 ( $00000000 - 01111111$ )<sub>2</sub>, el número de redes posibles es  $2^7 = 128 - 2 = 126$  redes. Se le

resta 2 pues uno de estos valores es un valor reservado y el otro es una restricción. La restricción es debido a que la dirección 0.0.0.0 fue definida originalmente como dirección de broadcast. El valor reservado es utilizado para pruebas y a esta red se le conoce como red Loopback (127.0.0.0) o bucle cerrado, esta red se utiliza para que un host, encaminador o cualquier otro dispositivo que tenga una interfaz pueda enviar paquetes hacia ellos mismos y pueda comprobar si está bien la interfaz o no. El número de host o estaciones por red es de  $2^{24} = 16,777,216 - 2 = 16,777,214$ . Se le resta dos, pues en cada red o subred, se debe tener una dirección que la identifique, además debe tener una dirección de multidifusión o como más comúnmente se le conoce dirección de broadcast.

En las direcciones clase B, el primer y segundo octeto son identificadores de red y el tercer y cuarto octetos son los identificadores de host. Las direcciones clase B comienzan por los bits 1 y 0 en su primer octeto, el rango de esta red es de 128 a 191 ( $10000000 - 10111111$ )<sub>2</sub>. El número de redes posibles es igual a  $2^{(6+8)} = 2^{14} = 16,384 - 2 = 16,382$  redes posibles, se restan dos debido a que existen dos redes que están reservadas (128.0.0.0 y 191.255.0.0). El número de host por red es  $2^{16} = 65,536 - 2 = 65,534$  estaciones.

En las direcciones clase C, el primer, segundo y tercer octeto son identificadores de red y sólo el último octeto es identificador de host. Estas direcciones comienzan con sus primeros tres bits del primer octeto con valores binarios de 110, es por ello que el rango de esta clase es de 192 a 223 ( $11000000 - 11011111$ )<sub>2</sub>. El número de redes posibles es igual a  $2^{(5+8+8)} = 2^{21} = 2,097,152 - 2 = 2,097,150$ , se le restan dos debido a que en esta clase también existen dos redes reservadas (192.0.0.0 y 223.255.255.0) y el número de hosts por cada red es de  $2^8 = 256 - 2 = 254$ .

La clase D, es una clase creada para permitir multicast en una dirección IP. Como se mencionó una dirección multicast es una dirección que permite direccionar paquetes enviados a dicha IP hacia grupos predefinidos de direcciones IP, esto quiere decir que un solo host puede transmitir los mismos paquetes hacia múltiples receptores de forma simultánea. Los primeros cuatro bits del primer octeto de esta clase deben ser 1110, es por ello que el rango de esta clase es de 224 a 239 ( $11100000 - 11101111$ )<sub>2</sub>. En esta clase el número de bits del identificador de host es de 28 bits.

La última clase es la clase E, la cual es una clase reservada por la Fuerzas de Tareas de Ingeniería de Internet (IETF), para propósitos de investigación. Los primeros cuatro bits de una dirección perteneciente a esta clase deben ser 1111, es por ello que el rango de esta clase es de 240 a 255 ( $11110000 - 11111111$ )<sub>2</sub>. El número de bits de identificador de host es de 28 bits al igual que la clase D.

### **2.5.3 Direcciones IP privadas y públicas**

Para que una red sea administrable y que cada dispositivo se pueda direccionar, es necesario que se asigne una única IP por cada dispositivo y esa dirección no sea repetida en toda la red. Debido a que Internet es el conjunto de varias redes, no se puede repetir una IP para dos o más estaciones que estén conectadas en Internet aunque pertenezcan a diferente red. Es por ello que la IEEE decidió definir dos tipos de direcciones IP, la primera son las direcciones privadas y la segunda son las direcciones públicas.

Las direcciones públicas son aquellas que se utilizan para direccionar estaciones que se conectan a Internet. Las direcciones públicas son exclusivas, pues estas son globales y están estandarizadas. En un inicio estas

direcciones eran asignadas por la InterNIC (Centro de información de la red Internet), pero después ésta desapareció y este trabajo ahora lo ejecuta la IANA (Agencia de asignación de números de Internet), esto es para que la asignación de IP públicas sea controlada y regulada cuidadosamente para garantizar que no se genere una asignación de una dirección repetida.

Las direcciones privadas son aquellas que se utilizan para direccionar estaciones en una LAN privada, la cual no tiene salida al Internet, o si la tiene es a través de un NAT (*Network Address Translation* o traducción de dirección de una red). Este tipo de direcciones sí se puede repetir en varias redes siempre y cuando dichas redes no tengan comunicación entre sí. Esta fue una solución inmediata al problema de la escasez de IP's públicas, pues dentro de una red la cual no tenga salida a Internet, no es necesario asignarles IP's públicas. Una red privada podría utilizar cualquier dirección IP definidas en las distintas clases que se mencionaron anteriormente, pero es recomendable que se escoja dicha dirección de acuerdo al número de estaciones que van a haber por red, al número de redes que se quiere formar y si tendrá salida a Internet o no. Es por ello que en el RFC 1918 se definieron tres bloques de direcciones IP privadas dependiendo del tamaño de la red (clase A, B o C). Estas direcciones no se encaminan hacia el backbone de Internet, su uso es exclusivo para redes privadas y tampoco se puede utilizar para direccionar estaciones en Internet. Las estaciones en las redes pueden ser divididas en tres categorías. En la primera categoría se encuentran todas las estaciones que no requieren el acceso a otra red ni a Internet, en esta categoría las estaciones pueden utilizar direcciones IP iguales entre diferentes redes. En la segunda categoría se encuentran las estaciones que necesitan acceder a aplicaciones como correo electrónico, un servidor FTP, Telnet, esto quiere decir que una red se pueda comunicar con otras redes, pero no necesita salir a Internet, en esta categoría las estaciones pueden utilizar direcciones IP que sean repetidas entre las

diferentes redes (si y sólo si no tiene comunicación con una estación en diferente red pero con la misma IP) y que solamente necesiten conectarse a un servidor como FTP y no establecer comunicación entre ellas. En la última categoría o categoría 3, se encuentran las estaciones que necesitan salir a Internet, en este tipo de categoría es necesario que cada estación tenga una única dirección IP, o pueden tener repetidas IP privadas, pero al momento de anunciarse en internet tienen que tener una IP pública única.

Las direcciones IP privadas son las que están dentro de la categoría 1 y las direcciones IP públicas son las que están dentro de la categoría 3. Las direcciones privadas reservadas por la IANA se muestran en la tabla VI.

**Tabla VI. Direcciones privadas**

<b>Rango</b>	<b>Número de direcciones</b>	<b>Prefijo</b>
10.0.0.0 – 10.255.255.255	1 red clase A	8
172.16.0.0 – 172.31.255.255	16 redes clase B	12
192.168.0.0 – 192.168.255.255	256 redes clase C	16

Estas direcciones son sólo para uso particular de una red interna y no deben de encaminarse a Internet, o sea los routers pueden encaminar dichas redes a otras redes dentro de una misma WAN donde se utilicen direcciones privadas, pero no pueden ser conducidas a Internet a menos que se utilicen otras técnicas en las cuales se convierten dichas IP's de privadas a públicas, tal como NAT y PAT (*Port Address Translation* o traducción de puertos de direcciones). Para utilizar dichas direcciones IP, no es necesario coordinarse con la IANA ni registrarse, pues son de uso común y general.

#### 2.5.4 División de redes en subredes

Se utiliza la división de una red en subredes para administrar las direcciones IP que se tienen en una red en particular, dado que con dicha división se logra segmentar toda una red grande en subredes más pequeñas para poder tener redes de un número reducido de hosts en una misma red. El precio que hay que pagar por una mejor administración de direcciones IP es el de perder dos direcciones IP por cada nueva subred. La división de redes es utilizada también debido a las pocas direcciones IP públicas que existen.

Para poder llevar a cabo dichas subredes, es necesaria una máscara de subred, la cual es una máscara no por defecto utilizada para poder tomar algunos bits del campo de host y convertirlos en bits de subred. Se menciona una máscara no por defecto, pues para las tres principales clases de redes, las respectivas máscaras por defecto se muestran en la tabla VII.

**Tabla VII. Máscaras por defecto**

Clase	Máscara (Prefijo)
A	255.0.0.0 (8)
B	255.255.0.0 (16)
C	255.255.255.0 (24)

El prefijo no es más que el número de bits con valor igual 1 utilizados para formar la máscara.

Por ejemplo, si se desea dividir una red clase C, en dos subredes, en lo que tenemos que enfocarnos es en el número de bits de subredes que se toman prestados del campo de host. Para el caso en que se desean 2

subredes, el número de bits tendrían que ser 2, pues  $2^2 = 4 - 2 = 2$  subredes. Obsérvese que se restaron 2, pues una subred es de identificación de toda la red (o subred cero) y la otra es de la de difusión (o broadcast), aunque en la actualidad estas dos subredes sí se pueden utilizar. Entonces la máscara tendría que ser como sigue:

255.255.255.0	Máscara por defecto para red clase C
255.255.255.192	Máscara de subred

255.255.255.192	En decimal
11111111.11111111.11111111.11000000	En binario

De la máscara por defecto vemos que para formar la máscara de subred se tomaron 2 bits del campo de host (cuarto octeto) los cuales ahora se denominan bits de subred. Al convertir el número binario 11000000 a decimal se obtiene 192.

Siguiendo con nuestro ejemplo, si nuestra dirección de red fuera 192.168.3.0 con máscara de subred 255.255.255.192 (ó prefijo 26), las subredes quedarían de la siguiente manera:

Red: 192.168.3.0  
 Clase: C  
 Máscara por defecto: 255.255.255.0  
 Máscara de subred: 255.255.255.192  
 Número de subredes: 2  
 Número de hosts por subred: 62



Primera subred utilizable:

Rango de IP's: 192.168.3.65 - 192.168.3.126

Identificador de subred: 192.168.3.64

Broadcast de subred: 192.168.3.127

Segunda subred utilizable:

Rango de IP's: 192.168.3.129 – 192.168.3.190

Identificador de subred: 192.168.3.128

Broadcast de subred: 192.168.3.191

El número de host por subred se obtuvo de  $2^6 = 64 - 2 = 62$  host por subred, se le restó dos, pues una IP es el identificador de la subred y el otro es el de broadcast de cada subred.

Nótese que no se utilizaron la primera ni la última subred, debido a lo que se mencionó, que son la subred cero y la de broadcast y que antes se reservaban, pero en la actualidad se pueden utilizar.

## 2.6 Enrutamiento y transporte

El enrutamiento es el proceso de mover paquetes o datagramas de una red a otra red usando para ello los enrutadores los cuales trabajan en la capa 3 del modelo OSI. Es importante recalcar nuevamente la diferencia entre un protocolo enrutado y un protocolo de enrutamiento. En nuestro enfoque el protocolo enrutado es IP y algunos ejemplos de protocolos de enrutamiento son OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*) y EIGRP (*Enhanced Interior Gateway Routing Protocol*). Un protocolo de enrutamiento es utilizado por los enrutadores para que dinámicamente puedan hallar todas las redes en la interred y asegurar que los demás enrutadores posean esta tabla de enrutamiento, así de esta manera pueda determinarse el camino que

debe seguir un paquete a través de toda la interred para poder llegar a su destino. Una vez que se conocen todas las redes, un protocolo enrutado es usado para enviar los paquetes del usuario.

Un enrutador también puede conocer las rutas hacia las diferentes redes estáticamente. Esto quiere decir que alguna persona definió por medio de comandos propios del enrutador, cuál debería de ser la ruta que el paquete debe de tomar cuando se dirige a una red destino. Este tipo de enrutamiento tiene sus ventajas y desventajas. Una ventaja podría ser que consume menos ancho de banda para conocer todas las rutas, y una desventaja podría ser que cuando se está trabajando con redes grandes, se vuelve bastante complejo poder configurar todas las rutas. Otra desventaja podría ser que si se cae un enlace, el enrutador no puede saber qué otro camino tomar, a menos que se haya configurado.

Para poder enrutar paquetes un enrutador debe de saber como mínimo la dirección IP destino, los vecinos de quien puede aprender las rutas hacia las distintas redes, las posibles rutas a todas las redes, la mejor ruta a cada red y como mantener y verificar la información de enrutamiento.

### **2.6.1 Protocolos de enrutamiento dinámico**

Un protocolo de enrutamiento es el esquema de comunicación entre routers. En un protocolo de enrutamiento dinámico si la red está directamente conectada al enrutador, entonces el enrutador ya conoce la red, pero si no está directamente conectada, entonces debe de hacer su tabla de enrutamiento. Una vez formada la tabla de enrutamiento y si ocurre algún cambio dentro de la red, el enrutador informa a todos sus vecinos de los cambios hasta que la red converja o sea hasta que todos los enrutadores de la red tengan la misma tabla

de enrutamiento. Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en la tabla de enrutamiento y descartan las que no son válidas.

En este punto, toma bastante relevancia el AS (*Autonomous System*) o sistema autónomo, que es un conjunto de redes que están bajo una administración común, el cual cuenta con sus propias reglas y políticas, y que comparten una estrategia de enrutamiento común hacia el exterior, esto significa que todos los routers dentro del mismo AS comparten la misma tabla de enrutamiento. Estos AS son asignados por la ARIN y es un número de 16 bits.

#### **2.6.1.1 IGP's**

Los IGP (*Interior Gateway Protocol*) son protocolos de enrutamiento interior, que se les denomina interior porque son los que se pueden utilizar dentro de un AS.

Los IGP's están clasificados en base a cómo funcionan sus algoritmos, pues existen algoritmos que se basan en la distancia los cuales se les denominan vector-distancias, también están los protocolos basados en el estado del enlace y la tercera clase son híbridos.

Los protocolos vector-distancia se les conocen también como protocolos basados en algoritmos Bellman-Ford. Este tipo de protocolo envía periódicamente la tabla de enrutamiento completa a los routers vecinos, con lo cual pueden mantener la topología de la red, en base a lo que cada router va observando en sus vecindades. Las tablas de enrutamiento incluyen información acerca del costo total de la ruta, la cual está definida por su métrica

y la dirección IP del primer router en la ruta hacia cada una de las redes. Algunos de estos tipos de protocolos son el RIP (*Routing Information Protocol*) o protocolo de información de enrutamiento y el IGRP (*Interior Gateway Routing Protocol*) o protocolo de enrutamiento de salida interior. RIP es un protocolo que utiliza como métrica el número de saltos y es un protocolo bajo estándares públicos. El IGRP es un protocolo propietario de la marca Cisco, y que su métrica está compuesta por la combinación de variables como retardo, ancho de banda, confiabilidad y carga.

Los protocolos estado de enlace también son conocidos como protocolos con algoritmos Dijkstras o SPF (*Shortest Path First*) o primero la ruta más corta. Con este protocolo, a diferencia del protocolo vector-distancia, en las tablas de enrutamiento se mantiene información más completa de toda la red, pues se tiene la información de los routers más lejanos y no sólo de los vecinos. Este tipo de protocolo utiliza los LSA (*Link State Advertisement*) o publicaciones de estado del enlace que envía cada router, con esto se genera una base de datos topológica de toda la red, y con el SPF se realizan los cálculos de cuál es la ruta más corta, y ya con este resultado se crea la tabla de enrutamiento. La base de datos de la topología de la red la genera cada enrutador y esta topología la hace en forma de árbol, teniendo como raíz el mismo y las ramas son todas las rutas posibles hacia cada subred. Pero todas estas bondades tienen un costo, dentro de los cuales podemos mencionar que carga el procesador, consume más memoria y ancho de banda.

OSPF (*Open Shortest Path First*), es un protocolo de enrutamiento basado en el algoritmo de estado de enlace SPF, el cual se basa en tomar la ruta más corta como primera opción. Este es un protocolo estándar abierto lo cual quiere decir que muchos fabricantes pueden hacer uso de él. Además es un protocolo escalable, el cual no está limitado a 15 saltos como RIP, lo cual lo hace muy útil

para redes grandes. Las redes OSPF grandes utilizan un diseño jerárquico, lo que quiere decir que varias áreas se conectan a un área de distribución (también denominada área cero o backbone). Es necesario crear áreas para que las tablas de enrutamiento que tenga cada router no sean muy complejas ni grandes. Además para reducir la cantidad de intercambios de la información de enrutamiento entre los distintos vecinos de una misma red, los routers OSPF seleccionan a un router designado (DR) y a otro router de respaldo (BDR) los cuales sirven como puntos de enfoque para el intercambio de información de enrutamiento. El DR actúa como portavoz del segmento de broadcast, enviando la información del estado del enlace a todos los demás routers OSPF del segmento a través de la dirección de multicast 224.0.0.5. OSPF selecciona la ruta más rápida (la de menor costo) y sin bucles en el árbol SPF como la mejor ruta. OSPF admite VLSM (*Variable Length Subnet Mask*) o máscara de subred de longitud variable, y por ello se le conoce como un protocolo sin clase.

IS-IS (*Intermediate System to Intermediate System*) es el otro protocolo de enrutamiento dinámico de estado de enlace, el cual hace uso también de SPF. Es un protocolo de gran escalabilidad y de rápida convergencia al igual que OSPF. IS-IS integrado puede trabajar con protocolos OSI, así como con protocolos IP. El funcionamiento es muy parecido a OSPF, pues los routers IS-IS envían paquetes hello para habilitar las interfaces y descubrir vecinos y así establecer las adyacencias. Los routers IS-IS forman paquetes LSP (*Link-State Packet*), basados en sus interfaces locales que tienen configurado IS-IS y de los prefijos aprendidos de los routers adyacentes. Estos LSP son enviados a los routers adyacentes vecinos, exceptuando del vecino de quien recibieron el LSP. En base a estos LSP se construye el árbol de la topología de la red y se utiliza SPF para calcular la ruta más corta dando como resultado la tabla de enrutamiento. Una diferencia de IS-IS con OSPF es que no existe un área 0, el backbone para IS-IS está formado por una colección de routers capa 2 los

cuales pueden estar en diferentes áreas. La capa 1 es la capa donde los routers tienen en su base de datos de estado de enlace información de su propia área, mientras que la capa 2 es donde los routers tienen en su base de datos de estado de enlace información únicamente del enrutamiento inter-áreas. Si se trabaja en el modo OSI los routers IS-IS no deben de configurarse en capa 2 sólo en capa 1, pero si se trabaja en áreas IP puras, los routers se pueden configurar capa 2.

### **2.6.1.2 EGP's**

Los EGP (*Exterior Gateway Protocols*) o también denominados protocolos de enrutamiento externo, son los encargados de proveer el enrutamiento entre sistemas autónomos. Este tipo de protocolo es el que utiliza un ISP (*Internet Service Provider*), y es el que se utiliza en los routers del corazón de internet. Un EGP necesita de un conjunto de información antes de comenzar su operación, una lista de routers vecinos, una lista de redes a ser publicadas como de acceso directo y el número de sistema autónomo del router local.

El BGP (*Border Gateway Protocol*), es un protocolo de enrutamiento externo robusto que se utiliza entre sistemas autónomos, debido a esto se convirtió en el protocolo más utilizado en toda Internet. Para lograr la escalabilidad a este nivel, BGP utiliza varios parámetros a los cuales se les denomina atributos, con esto logra definir las políticas de enrutamiento y mantener un ambiente estable de enrutamiento. Además para reducir el tamaño de las tablas de enrutamiento, BGP hace uso de CIDR (*Classless Interdomain Routing*). En las actualizaciones de las tablas de enrutamiento que se realizan entre vecinos, primero se debe de establecer una conexión TCP entre dichos vecinos y así únicamente cuando se produce un cambio en alguna ruta, estos cambios son anunciados a los vecinos.

Las rutas aprendidas vía BGP traen asociadas propiedades, las cuales son utilizadas para determinar la mejor ruta a un destino, cuando existen múltiples rutas hacia un mismo destino. Estas propiedades son los atributos de BGP que se muestran en la tabla VIII.

**Tabla VIII. Atributos de BGP**

ATRIBUTO	DESCRIPCION
Peso	Este es un atributo local de cada router, y la ruta con mayor peso, es la que se preferirá. Este atributo no es notificado a los vecinos.
Preferencia local	Atributo que indica el router de salida que se prefiere dentro de un AS. El mayor número de preferencia local es el que se elige. Este atributo sí se notifica a los vecinos dentro de un mismo AS.
Multi-salida discriminatoria (MED)	También denominado atributo métrica. Es una sugerencia hacia el AS externo, con respecto a la ruta que prefiere el AS que está haciendo el anuncio.
Origen	Este atributo indica como BGP aprendió una ruta en particular. Puede ser IGP o sea ruta aprendida dentro del mismo AS, EGP que significa que la ruta la aprendió vía EBGp (Exterior BGP), o Incompleta que significa que no se sabe cómo aprendió la ruta, posiblemente por una redistribución en BGP.
Camino AS	Este atributo es el número de AS que se agrega cuando una notificación de rutas atraviesa dicho AS. Los routers instalan en su tabla de enrutamiento, la ruta que tenga menos AS's agregados. Si un router ve su propio AS entonces rechaza la ruta notificada.

Siguiete salto	Este es la dirección IP que se utiliza para poder alcanzar al router que hizo la publicación. Entre vecinos EBGP este es la dirección IP del enlace que los conecta. Para vecinos IBGP se propaga el siguiete salto EBGP dentro del AS.
Comunidad	Este atributo aporta una forma de agrupación de los destinos, dichos grupos se les denomina comunidades. Estas comunidades se pueden aplicar a las decisiones de enrutamiento como la aceptación, preferencia y redistribución. Para configurarlos se utilizan mapas de enrutamiento. Existen comunidades predefinidas como No-export, No-advertise e Internet.

## 2.7 Seguridad necesaria en IPv4

En los inicios de las redes de computadoras, la seguridad no era un tema tan relevante, pero con el transcurrir del tiempo y que se han ido agregando millones de usuarios a Internet, el tema de seguridad ha adquirido importancia.

La seguridad en redes de computadoras implica tres requisitos que son:

- Secreto, el cual requiere que la información en una computadora sea accesible solo para lectura sólo por alguien autorizado.
- Integridad, la cual requiere que los recursos de una computadora sean modificados solamente por entes autorizados.
- Disponibilidad, la cual requiere que los recursos de una computadora estén disponibles a los entes autorizados.



El protocolo IP en sus inicios no contaba con una seguridad generalizada en la capa IP. Con el transcurrir del tiempo la seguridad se fue añadiendo en las capas de aplicación, tales como SSL (*Secure Socket Layer*) para aplicaciones WEB. En la actualidad se cuenta con una gran variedad de opciones de seguridad que inclusive se repiten en los distintos protocolos de aplicación, creando todo un grupo de nuevos problemas, tales como múltiples, diferentes e incompatibles funciones de gestión de llaves.

Una de las primeras soluciones y de mucha importancia para la seguridad en las redes es el cifrado, el cual es una transformación carácter por carácter o bit por bit, sin importar la estructura lingüística del mensaje. Otra solución fue la utilización de firewalls y listas de control de acceso. Pero aún con estas soluciones con ciertas limitaciones, se necesita una opción más completa, y es por ello que la IETF decidió trabajar en un protocolo de seguridad que trabajara en la capa IP, por lo cual nace IPsec el cual está definido en el RFC 2401; sin embargo, el desarrollo de IPsec en la actual versión de IP (IPv4) ha presentado dificultad en la protección de paquetes IP cuando se utiliza NAT, es por ello que el estudio de IPsec se verá cuando analicemos IPv6, para poder analizar los beneficios que se obtiene con IPv6.

### **2.7.1 Criptografía y sus algoritmos**

La criptografía viene del griego *kryptos* que significa ocultar y *graphos* que significa escribir, lo que literalmente significa escritura secreta. Existen dos técnicas fundamentales en uso, la primera es el cifrado convencional conocido como cifrado simétrico, y la segunda es el cifrado con clave pública conocido también como cifrado asimétrico.

El cifrado convencional o simétrico, se cuenta con una clave única secreta que es compartida por el emisor y receptor. Este tipo de cifrado fue el que se utilizó inicialmente, y tiene cinco tipos de ingredientes que son:

- Texto nativo, es el mensaje original que llega al algoritmo.
- Algoritmo de cifrado, este es el algoritmo que lleva a cabo transformaciones y sustituciones en el texto nativo.
- Clave secreta, es también una entrada al algoritmo, y es en base a éste que se hacen las sustituciones y transformaciones.
- Texto cifrado, es el resultado que se produce del algoritmo.
- Algoritmo de descifrado: Este es el algoritmo de cifrado pero al revés.

Los dos algoritmos de cifrado convencionales de bloque más importantes son, el DES (*Data Encryption Standard*) y el TDEA (*Triple Data Encryption Algorithm*).

El cifrado de clave pública, fue el primer avance revolucionario en el cifrado debido a que éste estaba basado en funciones matemáticas y no en sustituciones y transformaciones como el cifrado convencional. Este tipo de cifrado contiene seis ingredientes:

- Texto nativo, es el mensaje original.
- Algoritmo de cifrado, es el algoritmo matemático.
- Clave pública y privada, éste es el par de claves que se utilizan para el cifrado y para el descifrado respectivamente.
- Texto cifrado, es el resultado que se obtiene del algoritmo de cifrado.
- Algoritmo de descifrado, prácticamente tiene la función en forma inversa del algoritmo de cifrado.

En IPv4, se utiliza mucho la encriptación ya sea con el cifrado convencional o con el asimétrico, debido a la falta de seguridad del protocolo IP. Dicha seguridad es mejorada en su nueva versión IPv6, como se verá más adelante.

### **2.7.2 Protección de una red utilizando un contra-fuegos**

Otra solución que se dio para mejorar la seguridad en redes IP utilizando versión 4, fue la introducción de un contra-fuegos o firewall. Un firewall es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red de intrusos que vienen de Internet.

Un firewall tiene dos componentes: dos enrutadores que realizan filtrado de paquetes y una puerta de enlace de aplicación. El primer enrutador filtra los paquetes de entrada y si cumplen con el criterio de filtrado entonces los reenvía de manera normal, pero si no cumple entonces desecha dichos paquetes, igual trabajo realiza el segundo enrutador a excepción que este trabaja con los paquetes de salida de la red. El criterio del filtrado puede ser un bloque de direcciones IP que están autorizados para entrar, o posiblemente que algunos puertos o sockets de aplicación pueden estar autorizados y otros no. La otra parte del firewall es la puerta de enlace de aplicación, la cual está dedicada a examinar cada mensaje que entra o sale pero a nivel de aplicación, por ejemplo configurar una puerta de enlace de correo y con ello examinar los mensajes que entran y salen de la red para bloquear y aceptar ciertos tipos de mensajes.

En los enrutadores firewall de entrada y salida, se deben de utilizar ACL (*Access Control List*) o listas de control de acceso, con ello se logra conseguir tener el control del tráfico entrante y saliente de alguna parte específica de la red. Las ACL son muy útiles pues se pueden crear ACL's en base a la

dirección IP, el tipo de protocolo enrutado y el número de puerto, por cada interfaz del enrutador, tanto para el tráfico entrante como para el tráfico saliente.

## **2.8 IPv4 limitaciones a corto plazo**

La necesidad de la actualización del protocolo IP, surgió desde los años 1980s, cuando se pudo predecir en base al continuo crecimiento de Internet que se estaba dando en esa época.

En IPv4 se cuenta con la capacidad de poder direccionar  $2^{32} = 4,294,967,296$  hosts, con lo cual uno podría pensar que es suficiente para poder acomodar fácilmente cientos de millones de hosts hacia Internet. Sin embargo, esto funcionaría si las direcciones IP se distribuyeran de forma secuencial, lo cual no es posible debido a su forma jerárquica de direccionamiento. Como se mencionó una dirección IP consta de dos partes, la primera es el identificador de la red y la segunda es el host al cual identifica. Esta forma jerárquica de direccionamiento fue definida de esa manera para poder fácilmente encaminar los paquetes de un host a otro, pues en el enrutamiento primero se encamina el paquete hacia la red a la que le corresponde, según la IP, y luego ya que se ha llegado a la red, se dirige el paquete al host que le pertenece, según también la IP.

Con el escaseo de direcciones IP, la IANA empezó a asignar las direcciones IP de una manera más restrictiva, y para organizaciones grandes que solicitaban redes clase B, se les otorgaba y se les sigue otorgando, siempre y cuando estén bien justificadas, y sólo se les asigna quizá una subred de una clase B. Las redes clases C son las que más comúnmente son asignadas, pero éstas tienen la limitación que pueden funcionar para redes pequeñas. Esta

limitación de asignaciones de IP's públicas es una de las limitaciones más notables y críticas de IPv4, pero no es la única.

Una necesidad que surge con la evolución de las computadoras es la movilidad, pues inicialmente las computadoras eran grandes cuartos de equipos, y hoy día existen una gran variedad de computadoras portátiles las cuales necesitan poder conectarse en Internet. En IPv4 un avance en la movilidad es el DHCP, pero con este protocolo aún se continúa dependiendo de un solo punto de conexión a la red, pues el host se mueve de dicho punto y desea conectarse a la red en un punto que no es un punto de conexión de su ISP, entonces debe volver a realizar una nueva conexión con los datos de este nuevo ISP (Gateway, máscara de subred y DNS).

Debido al problema de que no existen muchas direcciones IP públicas, se decidió trabajar con subredes de las distintas clases de redes existentes, y con ello optimizar el espacio de direccionamiento. Además con las subredes se podía adaptar el esquema de direccionamiento a las necesidades de las redes de cada organización. Lamentablemente organizaciones que necesitaban una clase B y lo solicitaban tenían que esperar mucho tiempo para que se las asignaran o en el peor y más común de los casos no se las asignaban y lo que les podían asignar eran varias clases C, pero esto iba haciendo mucho más largas las listas de enrutamiento.

La limitante de que las tablas de enrutamiento se iban haciendo cada vez más largas, fue solucionado con una herramienta llamada CIDR. Las listas de enrutamiento habían estado creciendo enormemente, mientras más y más redes se agregaban, y esto se traducía en mucha más latencia para Internet, o lo que es lo mismo mucho más tiempo a que un paquete pudiera llegar a su destino, pues cuando el paquete llegaba a un router, se tenía que buscar en

toda la lista de enrutamiento cuál debía ser el siguiente salto para poder llegar a la red destino, y con el crecimiento que venía teniendo y sigue teniendo Internet las listas eran enormes. Con CIDR se logró solventar dicho problema, pues como es un enrutamiento sin clase, lo que significa que con esto se le indica al router que ignore la clase a la que pertenece una subred o lo que es lo mismo que se haga una supernet de las diferentes subredes, logrando así que la tabla de enrutamiento sea más pequeña, lo que se traduce como una mejora en el desempeño del enrutamiento y una menor latencia en todo Internet.

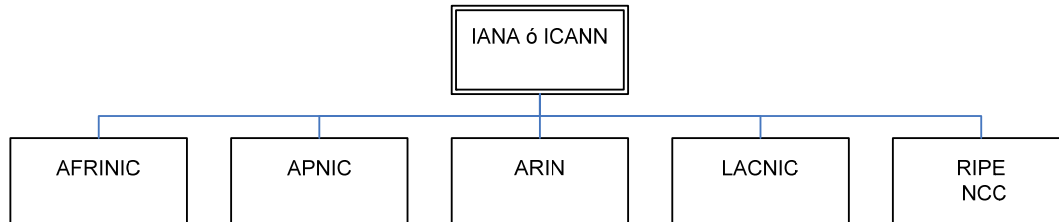
### 3. IPv6 LA SIGUIENTE GENERACIÓN

En el capítulo anterior se trató a profundidad el actual protocolo IPv4, detallando las características del mismo, así como las limitaciones que éste presenta. En el actual capítulo abordaremos a detalle el protocolo IPv6, así como también se verá la distribución actual de recursos de Internet, quién es la mayor autoridad y cuáles son los cinco registros regionales de Internet y cuáles son las áreas que éstas cubren.

#### 3.1 Distribución de recursos en Internet

La distribución de recursos en Internet en sus inicios fue controlada por la *Internet Assigned Numbers Authority* (cuyo acrónimo es IANA), y que en la actualidad a partir del año 1998 fue sustituido por la *Internet Corporation for Assigned Names and Numbers* (ICANN). Las atribuciones de la ICANN fueron dadas por el Departamento de Comercio de Estados Unidos bajo la figura de adjudicación directa y única. Las tareas de la ICANN fueron y siguen siendo la gestión de la asignación de nombres de dominio de primer nivel (el dominio de primer nivel es la parte final de un dominio de Internet, o sea las letras que siguen al punto final de cualquier nombre, por ejemplo el gt, edu, gob) y direcciones IP. Para estas tareas se crearon cinco RIR (Regional Internet Registry) o registros regionales de Internet, a las cuales la IANA delega los recursos para que sean éstas quienes sub-deleguen los recursos a los ISP y organizaciones de usuarios finales. Las cinco RIR son, ARIN, RIPE, APNIC, LACNIC y AFRINIC. El organigrama para la distribución de recursos en Internet se ilustra en la figura 36.

**Figura 36. Organigrama para la distribución de recursos de Internet**



La AFRINIC (*African Network Information Centre*) es la RIR que cubre la región de Africa y fue reconocida por la ICANN en abril de 2005.

La APNIC (*Asia-Pacific Network Information Centre*) es la RIR que cubre la región de Asia-Pacífico y fue fundada en enero de 1993.

La ARIN (*American Registry for Internet Numbers*) es la RIR que cubre las regiones de Canadá, varias islas en el caribe y Estados Unidos, que fue establecida en diciembre de 1997.

La LACNIC (*Latin American and Caribbean Internet Address Registry*) es la RIR que cubre las regiones de Latinoamérica y el Caribe que fue establecida en el año 2001.

La RIPE NCC (*Réseaux IP Européens Network Coordination Centre*) es la RIR que cubre las regiones de Europa, Medio Oriente y partes de Asia Central. Esta RIR fue establecida en abril de 1992.

### **3.2 ¿Por qué cambiar a un nuevo protocolo de Internet?**

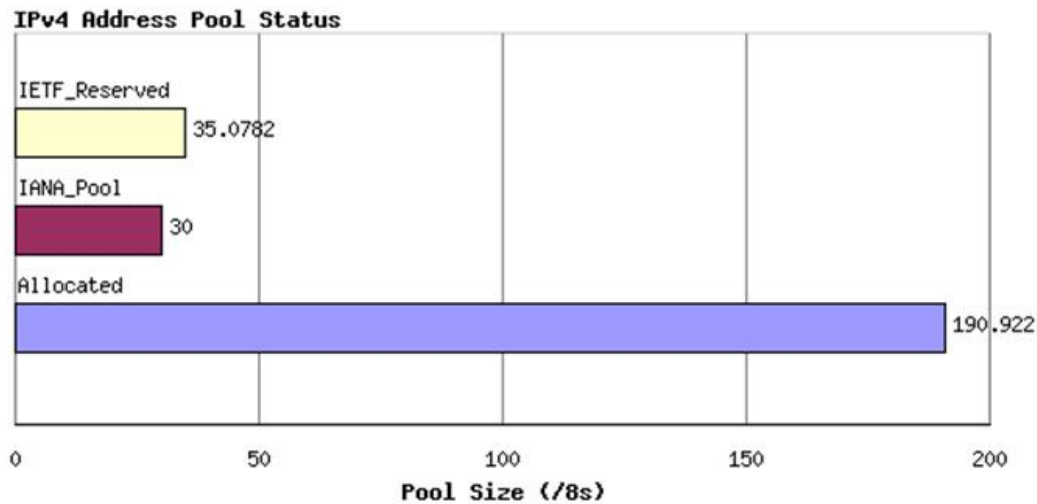
El criterio que utiliza la IANA para la asignación del espacio de direcciones IP a las distintas RIR, está descrito en documento denominado IPv4 Policy. El



espacio de direcciones IP es asignado en unidades “/8” que significan 1/256 parte del espacio total de direcciones IP. Para IPv4 el espacio total de direcciones IP  $2^{32} = 4,294,967,296$ , entonces un /8 sería igual a dividir la cantidad del espacio total de direcciones IP dentro de 256, lo cual daría un resultado de 16,777,216.

Como se menciona en el RFC 3330, un número de bloques de direcciones están reservados para usos no convencionales en lo relativo a Internet, tales como los bloques de identidad Unicast. Además, también se tienen reservados algunos bloques para usos específicos y el total de bloques reservados en unidades /8 es 36.086, el cual está compuesto por 16 bloques /8 reservados para multicast, 16 bloques /8 reservados para uso en el futuro, 1 bloque /8 para identificación de direcciones locales (0.0.0.0 /8), 1 bloque /8 reservado para loopback (127.0.0.0 /8), 1 bloque /8 reservado para uso privado (10.0.0.0 /8), y un bloque /8 reservado uso especial en las denominadas redes públicas (14.0.0.0 /8). Otros pequeños bloques también están reservados para usos específicos. Los restantes 219.914 bloques /8 están disponibles para uso público en Internet. IANA tiene asignada un grupo de direcciones, mientras que el resto ya han sido asignadas por IANA para su posterior asignación por el RIR. El estado actual del total de espacio de direcciones IPv4 se muestra en la figura 37:

**Figura 37. Estado a fecha 03/05/09 del espacio de direcciones IPv4**

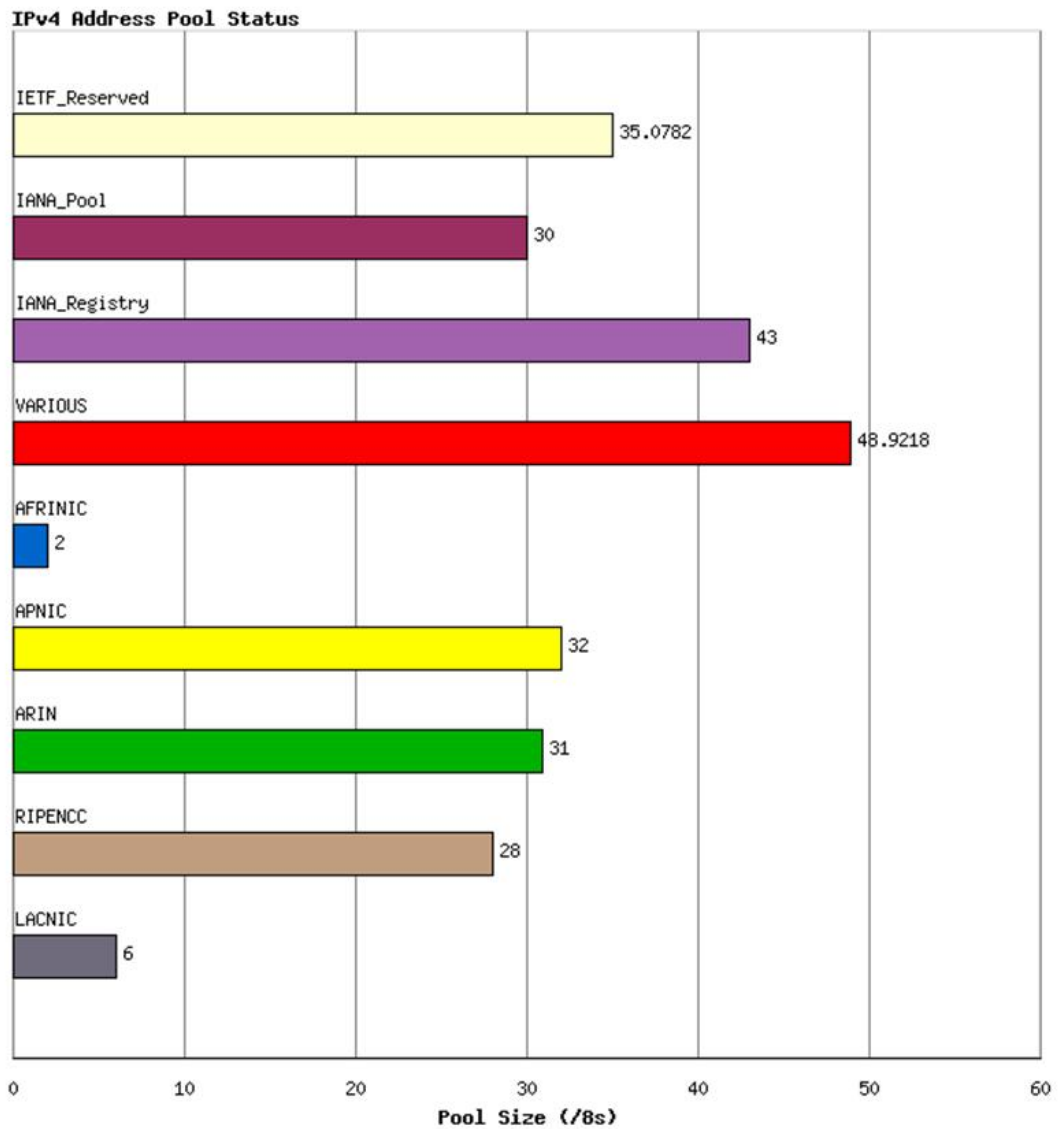


Este conjunto de direcciones mostrado en la anterior figura como “Allocated”, es administrado por las RIRs y el desglose de los bloques de direcciones asignadas por la IANA a cada una de las RIRs se muestra en la figura 38. El bloque denominado VARIOUS se refiere a las direcciones asignadas por la IANA antes que se estableciera el sistema de la RIRs.

Cualquier dirección IP individual puede estar en cualquiera de los siguientes 5 estados:

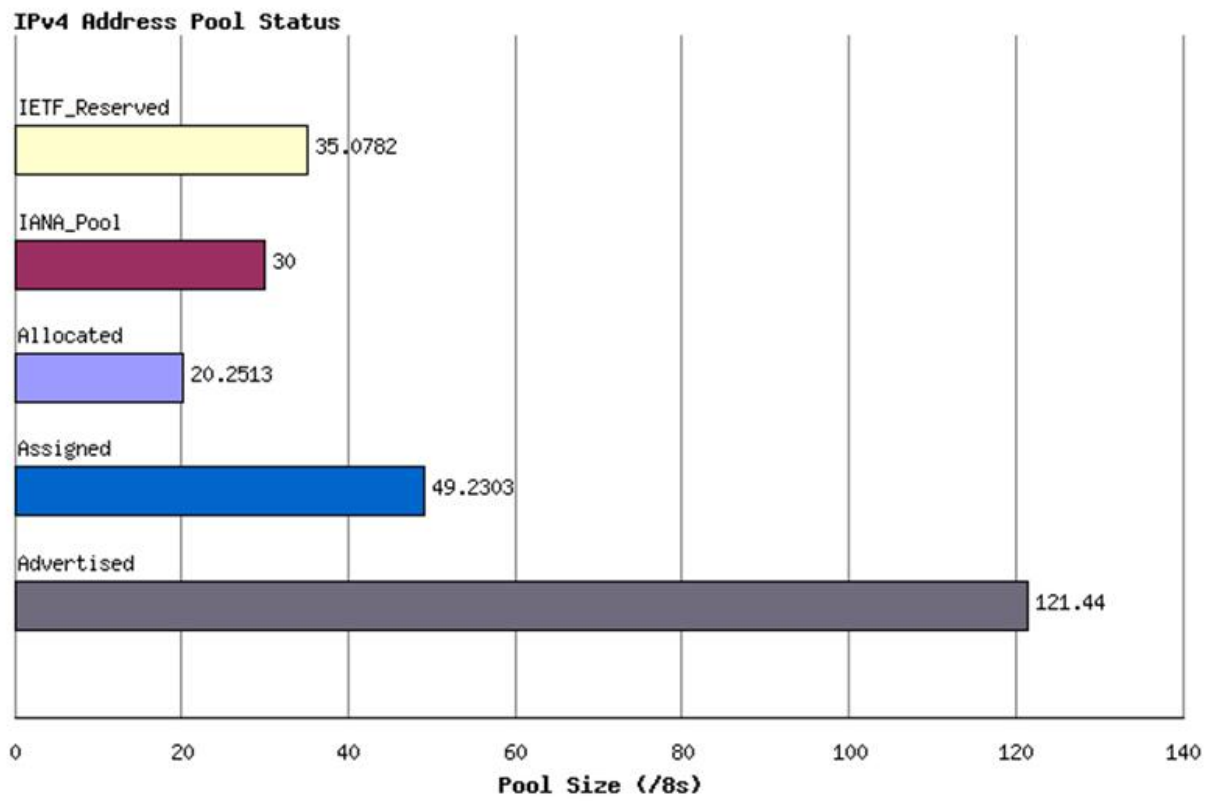
1. Reservados para uso especial (35.0782 bloques /8)
2. Parte de los bloques no asignados por la IANA (30 bloques /8)
3. Parte de la reserva no asignada en poder de un RIR (190.922 bloques /8 menos los asignados).
4. Asignados a un usuario final o entidad, pero que no están siendo anunciados en el sistema de enrutamiento.
5. Anunciados y publicados en las tablas de enrutamiento BGP.

Figura 38. Desglose de direcciones asignadas por IANA a RIRs



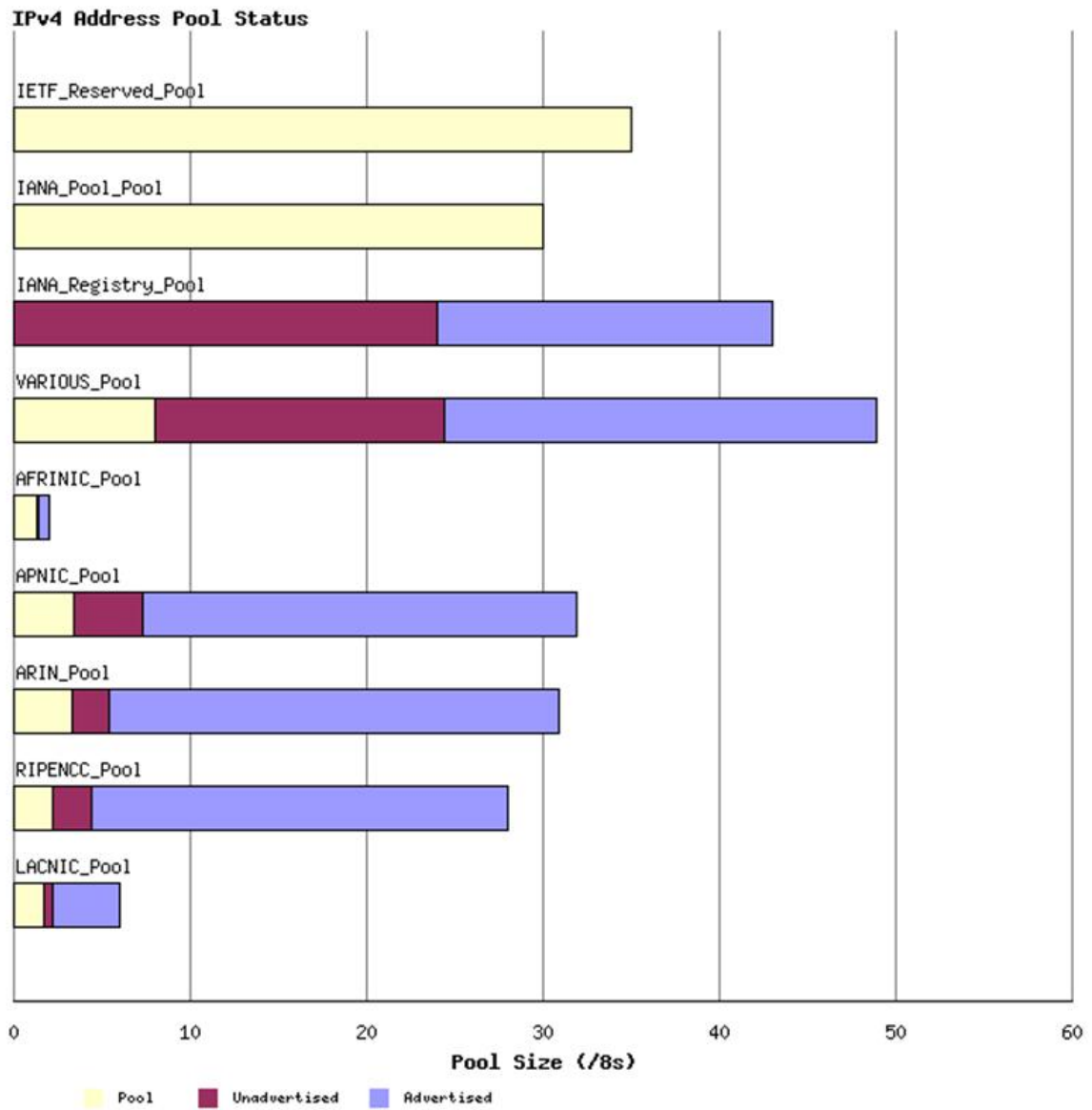
El estado actual de las direcciones IP de acuerdo con este conjunto de estados se muestra en la figura 39.

Figura 39. Estado de direcciones IP de acuerdo con conjunto de estados



Este estado puede ser categorizado por un RIR como se muestra en la figura 40.

Figura 40. Estado de direcciones IP categorizada por RIR



De acuerdo con proyecciones del investigador Geoff Huston, que toma como base el consumo pasado de IPv4, el cual hace un análisis de Series de Tiempo en su trabajo de investigación, llega a una conclusión con su modelo predictivo dinámico que:

- ✓ El agotamiento proyectado de las direcciones no asignadas por la IANA se dará el 12 de agosto de 2011.
- ✓ El agotamiento proyectado de las direcciones no asignadas por las RIRs se dará el 01 de mayo de 2012.

Estas predicciones hechas por el modelo de Huston, cambiarán el día de mañana, pues el modelo es un modelo dinámico. Además los supuestos que utiliza este modelo son:

- ✓ Que el mañana es muy parecido al hoy
- ✓ La tendencia que se observa hoy se observará mañana
- ✓ No habrá pánico
- ✓ No habrá cambios en políticas
- ✓ No habrá cambios en la dinámica de la demanda
- ✓ No hay externalidades
- ✓ No hay racionamiento ni retención.

Dado estas proyecciones del agotamiento de las direcciones IPv4, y que la demanda de direcciones IP ha ido incrementándose, se necesitará comenzar a migrar nuestras redes al nuevo protocolo IPv6 lo antes posible. Esto se debe de hacer pues la migración a IPv6 debe de estar realizada completamente antes que las direcciones IPv4 se terminen definitivamente.

### 3.3 Características y beneficios de IPv6

El diseño de IPv6 por parte de la IETF es una nueva versión del protocolo de Internet que fue diseñado como un paso evolucionario más que como un paso revolucionario de IPv4. Muchas de las buenas funcionalidades de IPv4 se mantuvieron y otras que no eran tan buenas fueron removidas, así como otras funcionalidades nuevas que fueron agregadas. A continuación se listan y detallan de manera breve algunas de las características de IPv6, que serán tratadas a mayor profundidad más adelante:

- Direcciones más largas, pasando de una dirección de 32 bits a una dirección de 128 bits, lo cual permite direccionar 340,282,366,920,938,463,374,607,431,768,211,456 nodos, eliminando así la necesidad de NAT.
- Más niveles jerárquicos de direccionamiento, lo cual provee una eficiente, jerárquica, y sumariada infraestructura de enrutamiento, o sea una mejor agregación de rutas.
- Arquitectura de direcciones simple y fija, lo cual permite una fácil planificación y con ello se reduce el costo de manejo de las redes. Ahora en IPv6 las máscaras de subred son fijas y proveen una virtual cantidad ilimitada de nodos en un enlace.
- Direcciones privadas, éstas están compuestas por bits específicos en la dirección para las redes que no van a estar conectadas a Internet. Estas son diferentes a las redes privadas IPv4 del RFC1918, pues en IPv6 estas direcciones permanecen únicamente asignadas a una red o a un nodo, lo cual hace que la conectividad entre redes privadas sea más fácil.

- Nodos autoconfigurables, esto está basado en los anuncios que envían los encaminadores, en la cual los nodos insertan su dirección MAC en la parte de la dirección de host en IPv6.
- No hay conflictos de direcciones en enlaces, esto es debido a que en la parte de host de IPv6 se incrusta una única dirección MAC que garantiza que no habrá otra dirección igual.
- Alcance del direccionamiento Multicast, que ahora en IPv6 se tiene un alcance del enlace que está dentro de la dirección Multicast, mientras que en IPv4 se tenía que confiar en el TTL.
- Una cabecera más simple y eficiente, pues ahora se cuenta con menos números de campos, no hay checksum, lo cual hace que los encaminadores procesen los paquetes más rápido y más eficientemente.
- IPSec obligatorio, en IPv6 se dice que la seguridad aumenta, debido que IPsec que en IPv4 era opcional para mejorar la seguridad, en IPv6 se vuelve obligatorio.
- Transición simple y flexible, este fue un requerimiento de que el nuevo protocolo fuera simple y flexible en su transición y con un bajo costo.
- Mejor soporte para QoS (*Quality of Service*), esto es debido a que hay nuevos campos en la cabecera IPv6 que definen cómo el tráfico se manejará e identificará en tiempo real, esto inclusive aunque el campo de carga útil esté encriptado. Esto es debido al campo de IPv6 que se llama "Flow Label" o Etiquetado de flujo.

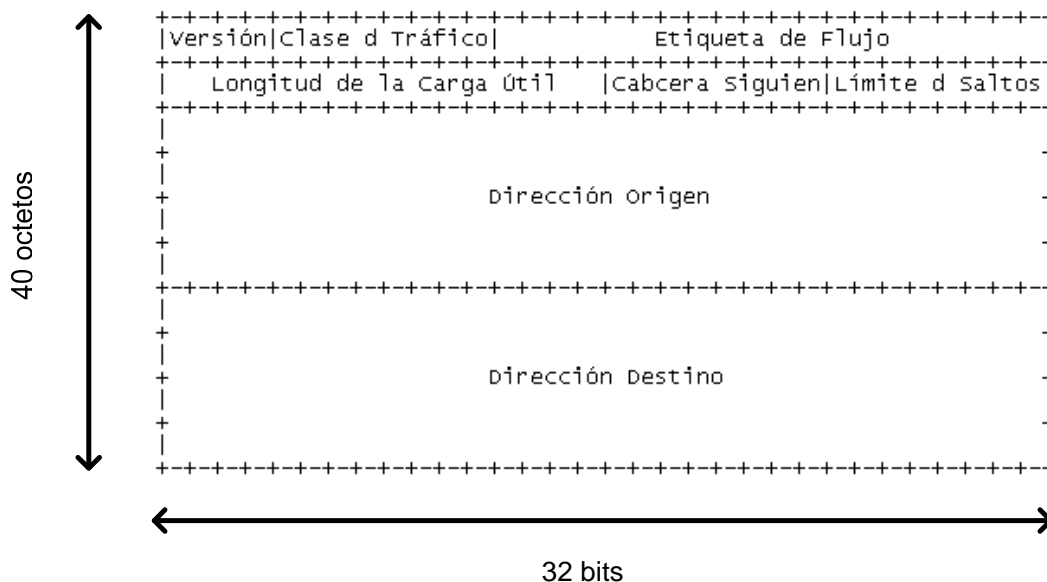
### 3.4 Formato de la cabecera IPv6

La cabecera básica IPv6 [RC2460] es más simple que la de IPv4, ésta tiene 8 campos en lugar de 12. El campo Longitud de Cabecera es removido así como el de Checksum, se agrega el campo Etiquetado de Flujo. De las extensiones son removidos los campos de fragmentación. El tamaño de la



cabecera básica es de 40 octetos, que es el doble de la de IPv4. Esto es debido en parte a que se incrementaron los campos Dirección origen y Dirección destino de 4 octetos a 16 octetos cada uno, o sea que el tamaño de las direcciones es 4 veces mayor. La cabecera IPv6 se muestra en la figura 41.

**Figura 41. Cabecera básica IPv6**



Fuente: RFC 2460, página 4.

Las extensiones de la cabecera son opcionales y van después de la cabecera básica mostrada en la figura 41. Son similares a las opciones en la cabecera de IPv4. Después de las extensiones de la cabecera, lo que sigue en la carga útil es la cabecera del protocolo de transporte.

### 3.4.1 Campos de la cabecera IPv6

El primer campo es el campo versión, el cual contiene 4 bits y que identifica la versión del protocolo IP. Este habilita al sistema operativo a transmitir a una pila adecuada, para IPv6 el valor es 6.

El segundo campo es el de clase de tráfico, el cual tiene 8 bits. Este era definido en IPv4 como tipo de servicio y los bits eran inicialmente asignados para identificar a los distintos tipos de niveles de servicios para los datagramas [RFC791]. La asignación de los bits fue redefinido, en el RFC2474, para diferenciar los servicios (diffserv) y los puntos de código (DSCP). Diffserv está compuesto de 6 bits y éste habilita la calidad de servicio en la red y los últimos 2 bits de ECN son utilizados para una notificación explícita de congestión. El campo clase de tráfico está disponible para usarse en los nodos originantes así como en los enrutadores reenviantes. Existen algunos requisitos generales que se aplican a este campo como lo son:

- 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.
- Los nodos que soportan un uso (experimental o estándar eventual) específico 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 cualquiera de los bits del campo Clase de Tráfico para los cuales no dan soporte a un uso específico.

- Un protocolo de capa superior no debe asumir que el valor de los bits Clase de Tráfico en un paquete recibido sean los mismos que el valor enviado por el origen del paquete.

El tercer campo es el de etiqueta de flujo, en IPv4 los enrutadores tenían que abrir la cabecera IP y la cabecera de transporte para poder identificar el flujo y posteriormente aplicar un procesamiento específico para la calidad de servicio. Esto introducía latencia y retrasos. Este campo está compuesto de 20 bits y es el único nuevo campo que se introdujo en la cabecera de IPv6. El host origen etiqueta el flujo poniendo un identificador de flujo en este campo de la cabecera, y esto habilita al enrutador para dar un procesamiento especial a todos los datagramas que vengan con esa etiqueta dado que tiene acceso directo a estas etiquetas. Los nodos que no soportan la función de este campo, deben de pasar el datagrama sin cambio alguno.

El cuarto campo es el de la longitud del campo útil, el cual está contenido de 16 bits, y define la longitud de lo que sigue después de la cabecera básica de IPv6, esto quiere decir que mide la longitud de la información del transporte, de la aplicación así como de las extensiones de la cabecera si hubieran. La máxima longitud del campo útil es de  $2^{16} = 65536$  octetos.

El quinto campo es el de siguiente cabecera el cual está compuesto de 8 bits. Este campo identifica los datos que están dentro de la carga útil del datagrama IP. Típicamente este es el protocolo de transporte (TCP o UDP) pero puede ser protocolos de encapsulamiento como ESP para IPsec. Este campo es el equivalente al del campo de Protocolo en IPv4 y comparte los mismos valores. El listado completo de los números de protocolos se puede encontrar en la página de IANA en la parte de números de protocolos.

El sexto campo es el de límite de saltos, el cual está compuesto de 8 bits, que fue implementado derivado de una sugerencia en el RFC791, como un contador de  $2^8 = 256$ , el cual va disminuyendo en una unidad cada vez que un enrutador envía el datagrama, hasta que su valor llega a cero, entonces se envía un mensaje ICMP de “tiempo excedido”.

El séptimo y octavo campo son de 128 bits cada uno, y corresponden al campo de dirección de origen y dirección destino. Estos campos tienen la misma función que en IPv4 con la única diferencia que son 4 veces más grandes.

### **3.4.2 Extensiones de la cabecera IPv6**

Las extensiones de la cabecera de IPv6 son una manera de manejar las opciones de IPv4 mejorando el procesamiento, estas extensiones se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior siguiente dentro de un paquete. Cada extensión de cabecera es un múltiplo de 8 octetos de largo, para conservar la alineación de 8 octetos para las cabeceras subsiguientes y cada uno de los tipos de extensiones están identificadas por un valor específico del campo siguiente cabecera, como se lista en la tabla IX.

**Tabla IX. Valores de siguiente cabecera para las extensiones IPv6**

<b>Valor</b>	<b>Descripción</b>
0	Opciones de salto a salto
43	Enrutamiento (tipo 0)
44	Fragmento
50	Seguridad del encapsulado de carga útil
51	Autenticación
59	Sin siguiente cabecera
60	Opciones de destino

Fuente: RFC 2460, RFC 2402

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. Las extensiones de cabecera se deben de procesar únicamente en el orden en que vienen. El valor de la siguiente cabecera de la cabecera del datagrama IP está apuntando a la primera extensión (si hubiera), y esta extensión apuntando a la siguiente y así sucesivamente. Es por ello que cuando más de una extensión de cabecera se usa en un mismo paquete, se recomienda que esas cabeceras tengan un orden el cual está especificado en el RFC 2460 y aparece en la tabla X.

**Tabla X. Orden de las extensiones de cabecera IPv6**

<b>Orden</b>	<b>Cabecera</b>
1	IPv6
2	Opciones de salto a salto
3	Opciones de destino (nota 1)
4	Enrutamiento
5	Fragmento
6	Autenticación
7	Seguridad del encapsulado de carga útil (nota 2)
8	Opciones de destino (nota 3)
9	De capa superior

Fuente: RFC 2460

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.

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.

#### **3.4.2.1 Salto a salto**

La opción salto a salto tiene que ser examinada por cada uno de los nodos intermedios, como por ejemplo enrutadores, que hay en todo el camino hasta el destino. Actualmente hay dos usos para esta extensión, la de alerta de enrutador y la de Jumbograma. La función de alerta de enrutador sirve para alertar a los nodos intermediarios que están a lo largo del camino para que procesen específicamente el datagrama, y así es una fácil manera en que los enrutadores pueden interceptar únicamente estos datagramas etiquetados sin sobrecargar el procesamiento de los mismos.

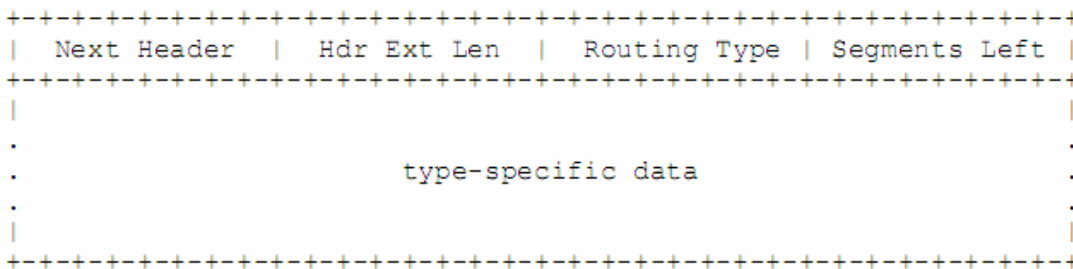
Los jumbogramas son datagramas de una longitud mayor de 64,000 octetos, los cuales necesitan de un procesamiento especial por todos los nodos intermedios como por ejemplo los enrutadores, debido a que son sobredimensionados comparados con el máximo de 16 bits de longitud del campo de carga útil. Un jumbograma es identificado por los siguientes campos:

- El campo de longitud de carga útil está fijo con un valor igual a 0.
- El campo siguiente cabecera está configurado con la opción salto a salto.
- La extensión salto a salto identifica a un jumbograma y contiene 32 bits especificando el tamaño del datagrama. De aquí que los jumbogramas tienen un tamaño máximo de 4Gigabits =  $2^{32}$ .

### 3.4.2.2 Enrutamiento

La cabecera de enrutamiento es una lista en la cual se indica cuál o cuáles son los nodos que se visitarán para alcanzar el destino del paquete, ésta es muy parecida a opción de origen impreciso y registro de ruta de IPv4. El valor de identificación de esta extensión es de una cabecera siguiente igual a 43 (NH=43) y tiene el formato que se muestra en la figura 42.

**Figura 42. Cabecera de enrutamiento**



Fuente: RFC 2460.

El campo cabecera siguiente identifica el tipo de cabecera que sigue inmediatamente a la cabecera de enrutamiento. El campo longitud de la extensión de la cabecera es un campo de 8 bits el cual mide la longitud de la cabecera de enrutamiento en unidades de 8 octetos. El campo de tipo de enrutamiento es un campo de 8 bits que identifica alguna variante en la cabecera de enrutamiento. El campo de segmentos pendientes es un campo



de 8 bits que indica el número de nodos intermedios explícitamente pendientes de visitar antes de alcanzar el destino del paquete. El campo de tipo específicos de datos es un campo de longitud variable que depende del campo de tipo de enrutamiento y del campo de longitud tal que la cabecera de enrutamiento completa es un número entero múltiplo de 8 octetos de longitud.

Si mientras se procesa un paquete recibido, el nodo encuentra una cabecera de enrutamiento con un valor de tipo de enrutamiento desconocido, el comportamiento de este nodo dependerá del valor del campo segmentos pendientes tal como sigue; si el valor del campo de segmentos pendientes es cero, el nodo debe de ignorar la cabecera de enrutamiento y proceder a procesar la siguiente cabecera del paquete. Si el valor del campo de segmentos pendientes no es cero, el nodo debe de descartar el paquete y mandar un mensaje ICMP “problema de parámetro” con código 0, al nodo que originó el paquete indicando el tipo de enrutamiento desconocido.

Habiendo procesado una cabecera de enrutamiento, si un nodo intermedio determina que el paquete recibido será remitido hacia un enlace cuya MTU es menor que el tamaño del paquete, dicho nodo debe de descartar el paquete y enviar un mensaje ICMP “paquete demasiado grande” a la dirección origen del paquete.

Una cabecera de enrutamiento no se examina o procesa hasta que alcance el nodo identificado en el campo de dirección destino de la cabecera IPv6. En dicho nodo al darle tratamiento al campo Siguiente Cabecera de la cabecera inmediatamente precedente ocasiona que la extensión cabecera de enrutamiento sea invocada.

### 3.4.2.3 Fragmento

La cabecera fragmento es utilizada por un origen IPv6 para enviar un paquete más grande que la MTU al igual que en IPv4, pero con la única diferencia que ésta se lleva única y exclusivamente por los nodos origen, y no puede ser realizada por los enrutadores a lo largo de la ruta de entrega del paquete, el nodo receptor es el encargado de hacer el ensamblaje. Esta cabecera se identifica con un valor de 44 en la cabecera inmediatamente precedente y el formato es el que se muestra en la figura 43.

**Figura 43. Cabecera fragmento.**



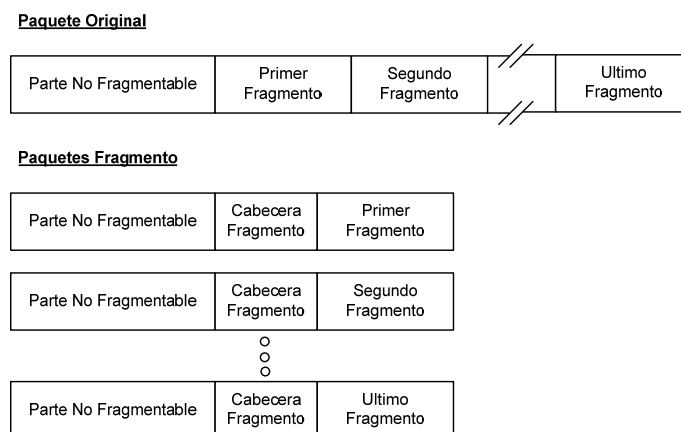
El campo siguiente cabecera, es de 8 bits, y es el que identifica el tipo de cabecera inicial de la parte fragmentable del paquete original. El campo reservado es de 8 bits, es un campo que se inicia en 0 para la transmisión y es ignorado en la recepción. El campo desplazamiento del fragmento es un entero sin signo de 13 bits, el cual indica el desplazamiento en unidades de 8 octetos de los datos que siguen a esta cabecera en relación al inicio de la parte fragmentable del paquete original. El campo Res, es un campo de 2 bits, el cual también es inicializado en 0 para la transmisión y es ignorado en la recepción. El campo M, es llamado Bandera M y es de 1 bit, el cual tiene como posibles valores 1= más fragmentos y 0=último fragmento.

El campo identificación es un campo de 32 bits, el cual es generado por el nodo origen para poder identificar a todos los paquetes que pertenecen al

paquete original. Este campo es usualmente implementado como contador el cual se incrementa en una unidad por cada paquete que necesita ser fragmentado por el nodo origen. La identificación debe de ser diferente a el de cualquier otro paquete fragmentado enviado recientemente (recientemente significa dentro del máximo tiempo de vida probable de un paquete, incluyendo el tránsito del origen hacia el destino y el tiempo gastado esperando el reensamblaje con otros fragmentos del mismo paquete) con la misma dirección origen y destino.

El paquete inicialmente sin fragmentar es llamado paquete original, el cual está compuesto de dos partes, la primera es la parte no fragmentable y la segunda es la parte fragmentable. La parte no fragmentable consiste de la cabecera IPv6 más alguna extensión que debe ser procesada por los nodos a lo largo de toda la ruta hasta alcanzar el destino. La parte fragmentable consiste en cualquier extensión de la cabecera que necesita ser únicamente procesada por el nodo destino más las cabeceras de capas superiores y cualquier otro dato. Los fragmentos se transmiten por separado en paquetes fragmento tal y como se observa en la figura 44.

**Figura 44. Paquete original y fragmentos**



El nodo destino reúne todos los fragmentos y los reensambla. Los fragmentos deben de tener la misma dirección de destino y de origen y el mismo valor de ensamblaje para poder reensamblarlos. Si todos los fragmentos no son recibidos por el destino dentro de los 60 segundos transcurridos después de haber recibido el primer fragmento, el nodo destino descartará todos los paquetes. Si el nodo destino ya había recibido el primer fragmento (el cual tendrá desplazamiento = cero), enviará de regreso al nodo origen un mensaje ICMPv6 “Tiempo de reensamblaje de fragmento excedido”.

#### 3.4.2.4 Opciones de destino

Esta cabecera es utilizada para llevar información adicional que va a ser examinada únicamente por el o los nodos destino del paquete. La cabecera opciones de destino es identificada por un valor de cabecera siguiente de 60 en la cabecera inmediatamente precedente y tiene el formato que se muestra en la figura 45.

**Figura 45. Cabecera Opciones de destino**

Siguiete Cabecera	Longitud Ext Cabecera	
Opciones		

El campo siguiente cabecera identifica el tipo de cabecera que sigue inmediatamente a la cabecera de opciones de destino.

El campo longitud de extensión de cabecera identifica la cabecera de opciones de destino en unidades de 8 octetos, la cual no incluye los primeros 8 octetos.

En el campo de opciones, puede haber una o varias opciones, y por lo tanto su longitud es variable y queda determinada de manera tal que es un entero múltiplo de 8 octetos de largo.

Un ejemplo de la extensión Opciones de destino, es IPv6 móvil.

#### **3.4.2.5 Autenticación y seguridad del encapsulado de carga útil**

Estas cabeceras son cabeceras del protocolo IPsec. Estas cabeceras son únicamente procesadas por el nodo destino. En el caso que existan túneles, la dirección destino apunta al final del túnel, mientras que internamente el datagrama apunta a un nodo final dentro de la red destino. En este caso el nodo destino que procesa la cabecera IPsec es el punto final del túnel.

IPsec para IPv6 es idéntico que para IPv4, lo único que IPv6 promueve más la utilización de éste debido a que ya no son usadas las NAT y además que en IPv6 es obligatorio utilizar IPsec.

#### **3.4.2.6 Sin siguiente cabecera**

Esta cabecera indica que no hay carga útil siguiendo esa cabecera. Esta aparece con un valor de 59 en el campo siguiente cabecera. Si el campo longitud de carga útil de la cabecera IPv6 indica la presencia de octetos más

allá del final de una cabecera cuyo campo cabecera siguiente contiene como valor 59, esos octetos deben de ignorarse.

### **3.5 Tamaño del datagrama en IPv6**

El tamaño del datagrama IPv6 depende del tamaño del MTU y del tamaño del campo de carga útil. El MTU es el máximo tamaño que una capa de enlace debe tener para poder soportar el datagrama.

Para cualquier enlace IPv4 requería un mínimo MTU en la capa de enlace de 68 octetos, mientras que el más eficiente MTU era de 576 octetos. 68 octetos es un MTU bastante bajo, dado que la mayoría de capas de enlace tienen un mínimo MTU de 1500.

En IPv6 el mínimo MTU es de 1280 octetos y el MTU más eficiente es de 1500 octetos. En cualquier enlace que no pueda llevarse un paquete de 1280 octetos en una pieza, debe proporcionarse fragmentación y reensamblaje. De cada enlace al cual un nodo se conecta, el nodo debe poder aceptar un MTU tan grande como grande sea el MTU del enlace.

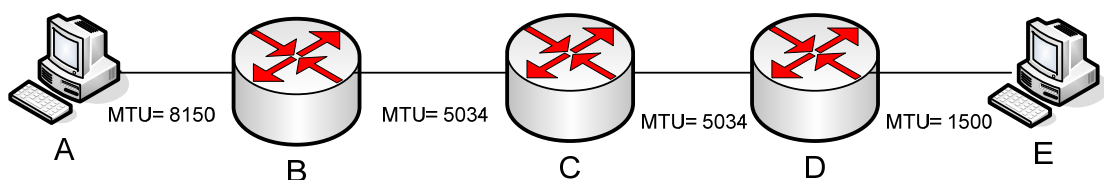
#### **3.5.1 Descubrimiento de la MTU de la ruta**

Es muy recomendable que los nodos IPv6 implementen el descubrimiento de la MTU de la ruta. Dado que los enrutadores no fragmentan los datagramas IPv6, si un datagrama es más largo que el tamaño de un enlace en la ruta hacia el destino del paquete, el enrutador que está conectado a ese enlace y que está recibiendo los datagramas, envía un mensaje de error ICMP a el nodo origen y el datagrama es descartado. Es por ello que los nodos IPv6 usan el descubrimiento de PMTU (Path MTU o ruta de la MTU) para poder descubrir el

MTU correcto a usar. El RFC que define el PMTU es el RFC1981 y ya se había definido para IPv4 como RFC1191 pero era raramente utilizado. Si no se utiliza esta opción, entonces el datagrama se envía con el mínimo MTU de 1280 octetos.

El proceso del descubrimiento de la MTU correcta de la ruta se muestra en la figura 46.

**Figura 46. Proceso de descubrimiento de MTU**



El proceso de descubrimiento de MTU de la figura 46, comienza cuando el nodo A envía un datagrama al destino E usando su propio MTU que es de 8150. El primer datagrama alcanza al enrutador B el cual no puede enviar el datagrama debido a que su MTU (5034) del siguiente enlace es más pequeña, por lo que envía un mensaje de error ICMP “paquete muy grande” hacia A con la MTU del siguiente enlace de B (5034) en el mensaje ICMP. Entonces el nodo origen A usa este MTU recibido de B y reenvía el datagrama a E con el nuevo MTU de 5034. El datagrama es reenviado por el enrutador B y C pero no por el D, pues el tamaño de MTU (1500) del siguiente enlace de D es muy pequeño, por lo que el enrutador D envía un mensaje de error ICMP al nodo origen A donde además también agrega su MTU del siguiente enlace. Entonces el nodo origen A recibe la nueva MTU enviada por el enrutador D, y reenvía el datagrama ahora con el nuevo MTU de 1500, y el datagrama llega exitosamente al nodo E. El nodo A selecciona el MTU de 1500 como el MTU para sus futuras comunicaciones con el nodo E.

Los nodos construyen una tabla con todas las MTU de las rutas para cada uno de sus destinos. El proceso de descubrimiento de rutas debe de estar realizándose periódicamente debido a que las topologías de las redes están cambiando dinámicamente a través del tiempo entre dos nodos, esto implica que PMTU esté cambiando también, y como los nodos no son informados cuando ocurren estos cambios, se debe de ejecutar el proceso de descubrimiento.

### **3.6 Direccionamiento en IP versión 6**

IPv4 es un protocolo que utiliza 32 bits para hacer el direccionamiento, con lo cual puede tener 4,294,967,296 direcciones IP. IPv6 es un protocolo que utiliza 128 bits con lo cual puede tener  $3.4 \cdot 10^{38}$  direcciones, lo cual es una de las mejoras que se tiene con IPv6. Para hacer un estimado de cuán grande es este número, tomemos como referencia la población mundial la cual está actualmente en aproximadamente 7 mil millones de habitantes, entonces con la cantidad de direcciones que se tiene en IPv6 se tendría un equivalente de  $4.8 \cdot 10^{28}$  de direcciones IPv6 para cada persona del planeta. La arquitectura de direccionamiento está descrito en el RFC 4291 que hizo obsoleto al RFC 3513.

Existen 3 tipos de direcciones IP:

- 1) Unicast: Esta es una dirección que identifica a una sola interface. Un paquete enviado a una dirección de este tipo es entregado a la interface que se identifica con esa dirección.
- 2) Anycast: Esta es una dirección que identifica a un grupo de interfaces que típicamente pertenecen a diferentes nodos. Un paquete enviado a una dirección de este tipo es entregado a una de las interfaces identificadas con esa dirección, y se entrega a la interface más cercana (en relación a métricas de distancia de los protocolos de enrutamiento).



- 3) Multicast: Esta es una dirección que identifica a un grupo de interfaces que típicamente pertenecen a diferentes nodos. Un paquete enviado a una dirección de este tipo es entregado a todas las interfaces identificadas con esa dirección.

### 3.6.1 Algunas reglas generales de las direcciones IPv6

Según el modelo de direccionamiento de IPv6, las direcciones IPv6 de todos los tipos son asignadas únicamente a las interfaces y no a los nodos, de tal manera que toda interface de un nodo necesita por lo menos de una dirección anycast. Una sola interface puede tener asignada múltiples direcciones IPv6 de cualquiera de los 3 tipos anteriormente listados. Un nodo puede entonces ser identificado por cualquiera de sus interfaces.

En IPv6 no existen las direcciones Broadcast que existían en IPv4, en su lugar ahora están las direcciones Multicast. Esta es una nueva y buena característica de IPv6, pues anteriormente el Broadcast era un problema en la mayoría de redes.

Una típica dirección IPv6 consiste de 3 partes, el prefijo de enrutamiento global, el identificador de subred y el identificador de la interface, los cuales se muestra en la figura 47.

**Figura 47. Formato general de una dirección IPv6**

Prefijo de enrutamiento Global Longitud= n bits	Subred ID Longitud= m bits	Interface ID Long= 128-n-m bits
---	-------------------------------	------------------------------------

Donde el prefijo de enrutamiento global es usado para identificar algunas de las direcciones especiales, tal como direcciones multicast. El ID de subred es el identificador de la subred o prefijo de subred en IPv4 y se utiliza para identificar el enlace al que pertenece el nodo. Un identificador de interface es usado para identificar una interface en un enlace y necesariamente debe haber una única en un enlace.

### **3.6.2 Formato de las direcciones en IPv6**

La técnica de representación de las direcciones en IPv6 es muy parecida al que se utiliza en el formato de IPv4. En IPv4 se utilizaban campo de 8 bits y cada campo estaba en sistema decimal. Ahora en IPv6 siempre se utilizan campos pero en sistema hexadecimal.

#### **3.6.2.1 Representación textual de las direcciones**

Las direcciones en IPv6 están representadas por 8 campos de números en base hexadecimal y cada campo está compuesto de 16 bits o sea 4 dígitos hexadecimales, separados en lugar de un “.” como en IPv4 por “:”. Algunas reglas que se pueden aplicar para hacer la representación de una dirección son las siguientes:

- a) No hay diferencia entre letras mayúsculas y minúsculas, por ejemplo “EF01” equivale a “ef01”.
- b) Es opcional dejar o no los ceros en un campo. Por ejemplo “00e1” es equivalente a “e1”.
- c) Una sucesión de ceros puede ser representada por “::” pero únicamente una vez en una dirección.

Por ejemplo la siguiente dirección:

00EF:0000:ABC9:0000:0000:1234:CDEF:0098

Puede ser representada usando la regla a), por:

00ef:0000:abc9:0000:0000:1234:cdef:0098

Que a la vez puede ser comprimida usando la regla b) por:

ef:0:abc9:0:0:1234:cdef:98

y que además usando la regla c) puede ser representada como:

ef:0:abc9::1234:cdef:98

Otros ejemplos de la regla c), son como los siguientes:

La dirección: 4DEF:0C00:0000:0000:0001:0000:0000:000E, puede ser representada como: 4DEF:0C00::1:0:0:E, en el cual se puede observar que sólo se pudo aplicar la regla c) una única vez en esa dirección.

La dirección: EF01:0000:0000:0000:0000:0000:0000:0001, puede ser representado usando la regla c) una única vez como: EF01::1.

La dirección 0000:0000:0000:0000:0000:0000:0000:000E, puede ser representado por la dirección ::E.

En ambientes donde existe una mezcla de nodos IPv4 e IPv6, una manera conveniente de tener una notación para las direcciones IPv4, es colocar la dirección IPv4 en los campos más bajos de la dirección IPv6. Por ejemplo, una dirección IPv4 192.168.0.2 puede ser representada en una dirección IPv6 x:x:x:x:x:192.168.0.2 y una dirección en la forma 0:0:0:0:0:0:192.168.0.2 puede ser reducida a una dirección ::192.168.0.2 o si se prefiere a la forma ::C0A8:2.

Con lo que respecta a las URLs (*Uniform Resource Locators*), que son las que usualmente contienen los nombres de los dominios, en IPv6 las direcciones en una URL deben de ir encerradas en corchetes “[ ]”, y para separar los puertos de las direcciones, se debe de hacer con “:”. Un ejemplo de ello podría ser:

Dirección: 00EF:0000:ABC9:0000:0000:1234:CDEF:0098

URL: http://[00EF:0000:ABC9:0000:0000:1234:CDEF:0098]:8080/test.html

### 3.6.2.2 Representación textual de los prefijos

Un prefijo representa un rango de direcciones. La representación textual del prefijo de la dirección IPv6 es muy similar a la manera en que se escribían los prefijos de las direcciones IPv4 en la notación CIDR. En un contexto en el cual se separa la parte de red y la parte del nodo, la longitud del prefijo representa el equivalente de una máscara de subred en IPv4. Un prefijo de una dirección IPv6 es representada por la notación:

Dirección IPv6 / longitud del prefijo

Donde la longitud del prefijo es un valor decimal que especifica cuantos de los bits contiguos que están más a la izquierda de la dirección comprenden el prefijo. El prefijo es usado para especificar la subred a la cual pertenece una interface y es usada por enrutadores para reenviar los paquetes.

Por ejemplo, para el prefijo de 60 bits 2009EDAB0000123 en hexadecimal, las siguientes representaciones son legales:

2009:EDAB:0000:1234:0000:0000:0000:0000 /60

2009:EDAB:0:1234::/ 60

2009:EDAB::1234:0:0:0 / 60

Pero no son legales las siguientes representaciones:

2009:EDAB:0:1234 /60, pues se pierden 4 campos de ceros

2009:EDAB::1234 /60, pues ésta al expandirla no da la misma dirección

Cuando se escribe la dirección del nodo y el prefijo, las dos pueden ser combinadas de la siguiente manera:

2009:EDAB:0000:1234:0000:0000:0000:0000 dirección del nodo

2009:EDAB:0:1234 /60 el identificador de la subred

De la manera abreviada: 2009:EDAB:0000:1234:0000:0000:0000:0000 /60

En la cual el prefijo 60 indica que la parte de red tiene 60 bits, y la parte del nodo los 4 restantes bits ( $128-60=68$  bits).

### 3.6.3 Identificación del tipo de dirección

Las direcciones Unicast son utilizadas para la comunicación entre dos nodos, mientras que las direcciones Multicast son usadas para la comunicación entre un nodo y muchos nodos y las direcciones Anycast son usadas para la comunicación entre un nodo y el nodo más cercano de entre un grupo de nodos.

El tipo de dirección IPv6 es identificada por los bits de más alto orden de las direcciones, como se muestra en la tabla XI.

**Tabla XI. Identificación del tipo de dirección IPv6**

Tipo de Dirección	Prefijo Binario	Notación IPv6
-------------------	-----------------	---------------

Sin especificar	00...0 (128 bits)	:: /128
Loopback	00...1 (128 bits)	::1 /128
Multicast	11111111	FF00:: /8
Enlace-local Unicast	1111111010	FE80:: /10
Unicast global	Cualquier otro	

Las direcciones Multicast comienzan con “FF” en el octeto de la izquierda. Cualquier otro valor en el octeto de la izquierda desde “00” hasta “FE” identifica a una dirección Unicast. Las direcciones Anycast no pueden ser distinguidas, pues estas son formadas utilizando el espacio Unicast.

### **3.6.4 Direcciones Unicast en IPv6**

Hay varios tipos de direcciones Unicast en IPv6 tales como Unicast global, sitio-local Unicast (aunque este tipo ya no se utiliza), enlace-local Unicast. También existen otros subtipos de Unicast global de propósito especial tales como direcciones IPv6 con direcciones IPv4 incorporados.

#### **3.6.4.1 Identificadores de interface**

Los identificadores de interface en direcciones IPv6 Unicast son usadas para identificar una interface en un enlace. Es requerido que sean únicas en un prefijo de subred. Es recomendado que el mismo identificador de interface no sea asignado a diferentes nodos en un enlace. Usualmente el identificador de interface se deriva de la dirección MAC, es por ello que se dice que las direcciones de los nodos IPv6 están basados en el formato IEEE EUI-64. El RFC 2373 incluye un apéndice donde se explica cómo crear los identificadores de interfaces. El mismo identificador de interface puede ser utilizado en

múltiples interfaces de un mismo nodo, mientras que las interfaces estén unidas a diferentes subredes.

Para todas las direcciones Unicast, exceptuando aquellas que comienzan con el valor binario "000", es requerido que los identificadores de interfaces tengan una longitud de 64 bits y que sean construidos en base al formato modificado EUI-34.

#### **3.6.4.2 Direcciones sin especificar**

La dirección con la forma 0:0:0:0:0:0:0 es llamada la dirección sin especificar, y nunca debe ser asignada a un nodo, pues ésta indica la ausencia de una dirección. Esta dirección tampoco debe ser utilizada como dirección destino ni en una cabecera de enrutamiento IPv6. Un paquete IPv6 con una dirección origen sin especificar nunca debe de ser reenviado por un enrutador.

#### **3.6.4.3 Direcciones Loopback**

En IPv6 estas direcciones están definidas como "0:0:0:0:0:0:0:1" o de manera simplificada como "::1". Esta dirección es utilizada para que un nodo IPv6 se envíe un paquete a sí mismo tal como en IPv4. Esta dirección no debe de ser usada como dirección origen en los paquetes IPv6 que son enviadas fuera de un nodo, y nunca debe de ser reenviado por un enrutador.

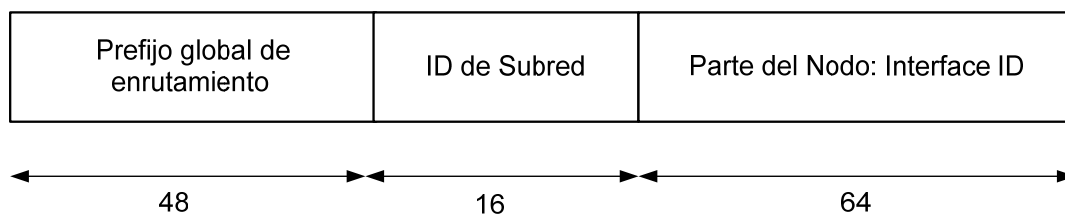
#### **3.6.4.4 Direcciones globales Unicast**

Las direcciones globales son utilizadas para comunicar los nodos con Internet. Estas direcciones, llamadas direcciones globales Unicast, están actualmente asignadas como "001" en los tres últimos bits de la izquierda de la

dirección. Esto corresponde a direcciones desde 2000:: hasta 3fff:ffff:ffff:ffff:ffff:ffff:ffff:ffff, o sea un espacio 2000:: /3. Este espacio de direcciones está definido para usar los 64 bits de la izquierda para el prefijo de la red y los 64 bits de la derecha para la parte de nodos. Esto quiere decir que, excepto en casos en que los bits de la izquierda empiecen con “000”, todas las subredes en IPv6 tienen el mismo prefijo de /64. Y esto se debe a que la parte del identificador de nodo es precisamente el identificador de interface, que como se mencionó es de 64 bits como la dirección MAC, debido a que está basado en el formato IEEE EUI-64.

El formato básico de una dirección global Unicast es mostrada en la figura 48.

**Figura 48. Formato básico de una dirección global Unicast**



Donde el prefijo global de enrutamiento tiene una longitud de 48 bits y el prefijo es asignado por el proveedor a un grupo de subredes o sitio. La parte del identificador de subred tiene una longitud de 16 bits y contiene los números de la subred dentro de un sitio,  $2^{16}$  subredes son permitidas. La parte de la derecha es de una longitud de 64 bits y contiene la parte del nodo, que también es llamada identificador de interface. Esta parte identifica el nodo dentro de una subred.  $2^{64}$  direcciones para nodos son permitidas en cada subred.



De lo anterior se puede decir que en IPv6, cualquier sitio, de cualquier tamaño, recibe un prefijo de "/48". Y todas las subredes, a excepción de algunos casos, tienen un prefijo fijo de "/64".

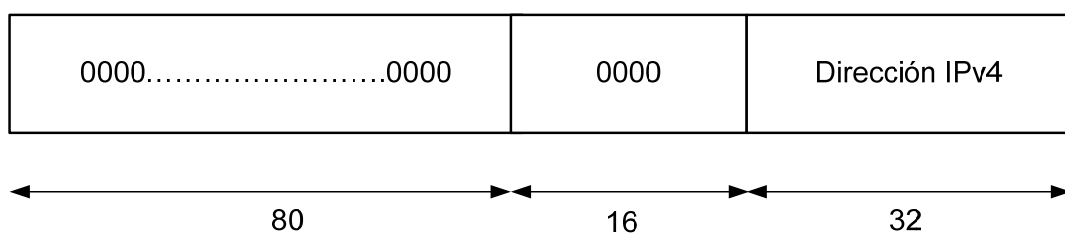
Con IPv6, todas las preocupaciones que se tenían con respecto a las restricciones y complicaciones con las máscaras de subred y la necesidad del espacio de direccionamiento, se han acabado, pues con IPv6 el plan de direccionamiento para un sitio se puede empezar enumerando cada una de las subredes que se tiene de las  $2^{16}$  permitidas. Cada una de estas subredes puede tener hasta  $2^{64}$  nodos, lo cual significa que no se necesita tener varias subredes para tener varios nodos en el mismo enlace.

### 3.6.4.5 Direcciones IPv6 con direcciones IPv4 insertadas

Existen dos tipos de direcciones IPv6 con direcciones IPv4 insertadas. La primera es direcciones IPv4 compatibles con direcciones IPv6 y la segunda son las direcciones IPv4 direccionadas como IPv6.

Las direcciones IPv4 compatibles con IPv6 fueron definidas con el propósito de ayudar en la transición a IPv6. El formato de este tipo de direcciones se muestra en la figura 49.

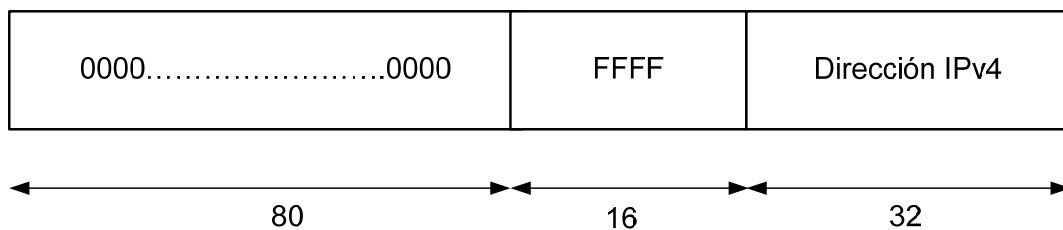
**Figura 49. Formato de una dirección IPv4 compatible con IPv6**



Las direcciones IPv4 deben de ser globalmente únicas. Este tipo de direcciones IPv6 ya no son actualmente utilizadas, pues se cuenta con nuevos mecanismos para la transición.

El segundo tipo de direcciones, direcciones IPv4 direccionadas como IPv6, son usadas para representar las direcciones de los IPv4 como direcciones IPv6. El formato de este tipo de direcciones se muestra en la figura 50.

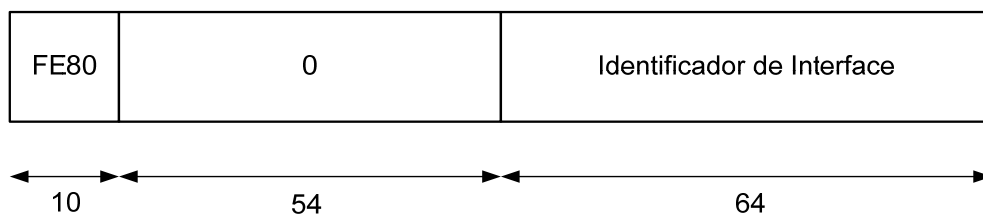
**Figura 50. Formato de una dirección IPv4 direccionada como IPv6**



#### 3.6.4.6 Direcciones Unicast IPv6 de enlace local

Las direcciones Unicast IPv6 de enlace local, son utilizadas únicamente para un solo enlace conectado a una interface, o sea que pueden ser utilizadas únicamente entre dos nodos en un mismo enlace y nunca son reenviadas por enrutador. El formato de dicho tipo de dirección se muestra en la figura 51.

**Figura 51. Formato de una dirección Unicast IPv6 de enlace local**



Este tipo de direcciones son automáticamente configuradas en cada interface IPv6 habilitada usando el formato IEEE EUI-64.

### **3.6.5 Direcciones Anycast en IPv6**

Como se mencionó este tipo de direcciones permite enviar un datagrama a un nodo que pertenece a un grupo de nodos que puede estar en la misma subred o topológicamente en diferentes enlaces de una red, con la propiedad que ese datagrama que es enviado a una dirección Anycast es enrutada a la interface más cercana que tenga dicha dirección, de acuerdo a las métricas de distancia de los protocolos de enrutamiento.

El mecanismo Anycast es usado para descubrir los servicios en una red o para proveer una redundancia. Un posible futuro uso de las direcciones Anycast es para identificar el conjunto de enrutadores que pertenecen a una organización que provee el servicio de Internet. Otro posible uso es para identificar el conjunto de enrutadores que pertenecen a una subred en particular.

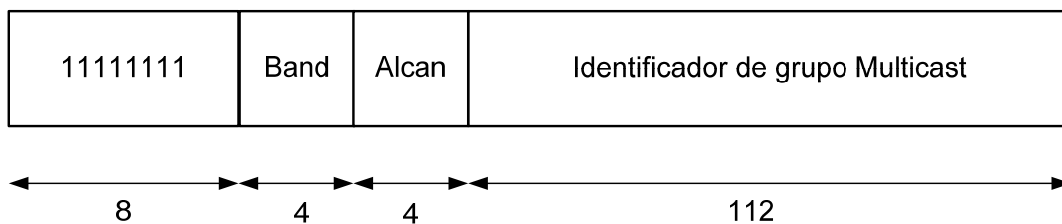
### **3.6.6 Direcciones Multicast en IPv6**

Una dirección IPv6 Multicast es un identificador de un grupo de interfaces. Multicast permite hacer un uso eficiente del ancho de banda al enviar un número mínimo de datagramas a un número máximo de nodos, es un mecanismo de direccionamiento de uno a varios. Un prefijo especial identifica a un datagrama multicast, y una dirección especial dentro de ese prefijo identifica a cada grupo de nodos.

IPv4 utiliza el Broadcast para varios propósitos. En su lugar IPv6 utiliza Multicast. Este permite enviar datagramas con objetivos más específicos a varios nodos en una red. Por ejemplo, los enrutadores IPv6 intercambian información específica usando una dirección específica en todos los enrutadores.

El formato de una dirección Multicast se muestra en la figura 52.

**Figura 52. Formato de una dirección Multicast**



Una dirección Multicast IPv6 debe iniciar con un valor hexadecimal de "FF" en su primer octeto.

El siguiente campo, es el campo denominado Banderas, el cual contiene una bandera de 1 bit que se utiliza para identificar el tiempo de vida del grupo Multicast. Si el valor es "0000", esto indica que es una dirección Multicast permanentemente asignada "bien conocida". Si el valor es "0001", esto indica que es una dirección Multicast temporalmente asignada. De los otros tres bits restantes del campo banderas, el que está más a la izquierda debe tener valor cero, y los dos bits siguientes (denominados bandera R y bandera P respectivamente) su definición y uso puede ser encontrado en el RFC 3306 y en el RFC 3956.

El campo Alcance, el cual es de 4 bits, es utilizado para limitar el alcance de un grupo Multicast. Los valores que puede tomar este campo se muestra en la tabla XII.

**Tabla XII. Valores del campo Alcance**

Valor en Hexadecimal	Alcance	Descripción
1	Interface local	Abarca solo una interface de un nodo
2	Enlace local	Abarca la misma región topológica que una Unicast
4	Admin-local	Es la de menor alcance y debe ser configurado manualmente.
5	Sitio-local	Destinado a abarcar solo un sitio.
8	Organización local	Destinado a abarcar varios sitios de una misma organización
0 / 3 / F	Reservado	
Cualquier otro valor	Sin asignar	Disponibles para que los administradores puedan definir regiones Multicast adicionales.

El último campo es el Identificador de grupo Multicast, el cual identifica al grupo ya sea permanente o temporal con su alcance respectivo. Otras definiciones de este campo se pueden encontrar en el RFC 3306.

### 3.7 Enrutamiento en IPv6

El enrutamiento en IPv6 es el proceso mediante el cual se mantiene una tabla de enrutamiento actualizada ya sea manualmente o dinámicamente tal y

como se hace en IPv4. Para enviar un paquete IPv6 más allá de los medios de comunicación locales se requiere de un enrutador. Los enrutadores verifican la dirección destino del paquete IPv6 y buscan el prefijo que le corresponde dentro de su tabla de enrutamiento. Una vez que el enrutador haya encontrado el prefijo para llegar al destino, entonces el paquete es reenviado de acuerdo con la información del siguiente salto. Si los enrutadores no encuentran la correspondencia en su tabla de enrutamiento, entonces el paquete es desechado.

Al igual que en IPv4, el enrutamiento en IPv6 se puede hacer estático o dinámico, y dentro del enrutamiento dinámico existen los mismos protocolos de enrutamiento pero con algunas modificaciones necesarias para poder soportar el nuevo protocolo IPv6.

La parte de configuración para el correcto enrutamiento en una red que utiliza IPv6 va a ser visto con detalle más adelante.

### **3.7.1 Rutas estáticas**

Las rutas estáticas son utilizadas para hacer el enrutamiento forzado de algunos prefijos a través de enrutadores específicos. Las rutas estáticas tienen la mayor preferencia en una tabla de enrutamiento sobre las rutas aprendidas por los protocolos dinámicos.

Una ruta estática contiene el prefijo a ser enrutado y la dirección IP del enrutador, el cual es llamado siguiente salto, responsable de enrutar cualquier paquete con un destino que esté dentro del rango del prefijo establecido. Un ejemplo de rutas estáticas es la ruta por defecto en IPv6 “::/0”.

Las rutas estáticas no han cambiado en IPv6, sin embargo una dirección enlace-local debe ser usada como dirección del siguiente salto.

### 3.7.2 RIP

RIP (*Routing Information Protocol*) es un protocolo de enrutamiento dinámico IGP que normalmente se utiliza en una red de tamaño mediano. La versión para IPv6 llamada RIPng (*RIP next generation*), es una versión mejorada de RIPv2 la cual tiene las mismas características como el utilizar el algoritmo de Bellman-Ford para la distancia-vector, cada 30 segundos hace una actualización de su tabla de enrutamiento, tiene métricas fijas, su alcance son 15 saltos.

Los cambios que sufre RIP para IPv6 se describen a continuación:

- Rutas publicadas. RIPng publica las rutas IPv6 en una manera compuesta por el prefijo IPv6, la longitud y la métrica.
- Siguiendo salto. La dirección del siguiente salto es la dirección IPv6 de enlace-local de la interface del enrutador que está publicando el prefijo.
- Protocolo de transporte. IPv6 utiliza UDP como protocolo de transporte para los datagramas RIP. Otro cambio es que el puerto que utiliza para UDP es el 521 en lugar del 520 como lo hacía RIP y RIPv2.
- Dirección origen IPv6. La actualización de la dirección origen IPv6 es la dirección enlace-local de la interface originante.
- Dirección destino IPv6. La actualización RIP de la dirección destino IPv6 es FF02::9, la cual es una dirección Multicast que es escuchada únicamente por enrutadores con RIPng configurado.
- Límite de saltos. Los paquetes IPv6 de actualizaciones RIP tiene un límite de saltos configurado de 255.

- Entradas enrutamiento. La entrada de enrutamiento IPv6 está separada de la entrada de enrutamiento IPv4 que se utiliza para RIPv1 o RIPv2. La ruta por defecto es anunciada como “::/0”.
- Autenticación. En IPv4 las dos versiones de RIP tenían su autenticación específica, en RIPv6 la autenticación está basada en IPsec.

### 3.7.3 OSPF

El OSPF (*Open Short Path First*) que se utiliza para IPv6 es conocido como OSPFv3, el cual comparte los mismos fundamentos que el OSPFv2 que se utiliza para IPv4.

Varios cambios fueron introducidos para que OSPFv3 pudiera soportar el nuevo protocolo enrutado IPv6, tales como:

- LSAs de la red y del enrutador. Estos LSAs (*Link State Advertisements* o anuncios de estado del enlace) sólo tienen información de la topología de la red.
- Nueva LSA Intra-Area-Prefijo. Este anuncio lleva la dirección IPv6 y los prefijos.
- Direcciones en LSA. Estas son descritas como prefijos con una longitud de prefijo.
- Identificador del enrutador. Todavía cuenta con 32 bits, pero ahora define si cuenta con direcciones IPv4 o IPv6. Este es usado en DR, BDR y LSAs.
- Alcance de las inundaciones. El enlace o un sistema autónomo.
- Siguiendo salto. La dirección del siguiente salto es la dirección IPv6 enlace-local de la interface del enrutador que está haciendo el anuncio.



- Nueva LSA de enlace-local. Este anuncio lleva la dirección enlace-local de la interface del enrutador, el prefijo del enlace y las opciones.
- OSPF corre ahora en un enlace completo y no sólo en una subred como sucedía en IPv4
- La dirección IPv6 origen de los paquetes OSPF es la dirección enlace-local de la interface del enrutador que origina el paquete.
- La base de datos del estado del enlace debe de ser doble, una de OSPFv2 para la red IPv4 y una base de datos OSPFv3 para la red IPv6 y su respectiva topología, a esto se le denomina “ships in the night” o “buques en la noche” .
- Todos los enrutadores OSPF envían paquetes Hello y escuchan la dirección multicast FF02::5. Los enrutadores designados y el de backup DR envían y escuchan la dirección multicast FF02::6.
- El límite de saltos de los paquetes OSPF es igual a 1.
- La autenticación de OSPF está basada en IPsec al igual que RIPng.

#### **3.7.4 IS-IS**

IS-IS (*Intermediate System to Intermediate System*) es un protocolo IGP de enrutamiento dinámico de estado de enlace que fue diseñado como un protocolo de enrutamiento independiente. IS-IS fue fácilmente adaptado para IPv6 únicamente añadiendo un pocos valores-tipo-longitud (TLV). Dado a que no hubo cambios de mayor magnitud en el protocolo IS-IS propiamente, no se tuvo que hacer una nueva versión del protocolo para soportar IPv6.

Debido a que IS-IS utiliza una encapsulación de capa 2, no es necesaria una dirección IP en el paquete. La implementación de IS-IS es considerada más fácil que la de OSPFv3.

Algunos de los pequeños cambios que sufrió IS-IS para poder soportar IPv6 se detallan a continuación:

- Un nuevo TLV tipo 236 de IPv6 alcanzable, el cual no es más que un aviso de ruta IPv6 el cual contiene el prefijo IPv6, la longitud del prefijo, la métrica e información adicional.
- Un nuevo TLV de dirección IPv6 de la interface (tipo=232), el cual para paquetes Hello es la dirección enlace-local del enrutador.
- Un IPv6 NLPID (*Network Layer Protocol Identifier*) con valor 142, el cual es enviado por los enrutadores para anunciar el soporte del enrutamiento IPv6 para IS-IS.

La base de datos de IS-IS de la topología de la red IPv4 y de la topología de red IPv6 deben de ser idénticas en un escenario integral de IS-IS, pero al igual que con OSPFv3, las bases de datos pueden ser diferentes, para cada topología de red, utilizando el concepto de “buques en la noche”.

### **3.7.5 BGP**

BGP (*Border Gateway Protocol*) es un protocolo utilizado para intercambiar rutas entre distintos dominios administrativos llamados sistemas autónomos (AS), como se había descrito en el capítulo anterior. Cuando BGP es usado entre distintos proveedores para intercambiar rutas se le llama BGP externo (eBGP). Cuando es usado dentro de un sistema autónomo se le llama BGP interno (iBGP).

El BGP Multiprotocolo (MBGP) es una versión extendida de BGP creada para soportar múltiples protocolos de red o familias de direcciones. Una nueva

familia de direcciones en MBGP es definida para IPv6 (RFC2545). Esta versión de BGP que soporta IPv6 fue llamada BGP4+ (RFC 4271).

Algunos de los cambios realizados sobre MBGP para poder soportar IPv6, se listan a continuación:

- Como siguiente salto en MBGP para IPv6, se puede configurar una dirección IPv6 ya sea global o de sitio.
- Con lo que respecta a NLRI (*Network Layer Reachability Information*) la ruta anunciada, es expresada como un prefijo IPv6 con su respectiva longitud.
- Se cuenta con una nueva dirección de familia para identificar las rutas IPv6.



## **4. ESTRATEGIA DE MIGRACIÓN A IPv6 Y SEGURIDAD QUE CONLLEVA**

En el capítulo anterior se abordó con detalle el nuevo protocolo IPv6, se vio cuáles eran sus características propias, cuáles son sus beneficios con respecto a IPv4, y todo lo necesario para poder entender cómo funciona dicho protocolo. Se está ya en la posición de poder ver cuál podría ser la estrategia de migración así como la seguridad que podría agregar IPv6 en nuestras redes.

En este capítulo se verá a detalle cuáles son esas posibles estrategias de migración para una red modelo estándar, se darán algunos ejemplos de configuraciones necesarias en equipo marca Cisco, sistema operativo Windows, y además se describirá cuál es la seguridad que agrega u obliga a tener el nuevo protocolo IPv6.

### **4.1 Seguridad que conlleva la migración a IPv6**

En el momento en que nuestras redes migren a IPv6, la seguridad que puede conllevar dicha migración es que en IPv6 es obligatorio configurar IPsec (IP Security o seguridad IP). Esto quiere decir que en toda red, ya sea migrada a IPv6 o que haya sido creada con IPv6 originalmente, IPsec tiene que ser obligatoriamente configurado, esto hace que se incremente la seguridad con relación al antiguo protocolo IPv4. Debido a este requerimiento la implementación de seguridad de IPsec se vuelve más fácil al realizarlo en IPv6.

Este requerimiento que IPv6 lleve obligatoriamente IPsec fue identificada como requisito clave por la IETF cuando estaban trabajando en los requerimientos de IPv6. IPsec (RFC 2401 actualizado por RFC 4301) fue diseñado para usarse tanto en IPv4 como en IPv6.

Algo importante que si hay que tomar en cuenta, es que este tipo de seguridad que agrega IPv6 es una seguridad únicamente en la capa IP (modelo TCP/IP) o capa de red (modelo OSI) y no es una arquitectura de seguridad para Internet. Es por ello que algunas de las políticas de seguridad que se utilizan en IPv4, como por ejemplo los filtrados de los firewalls o contrafuegos se deben de aplicar en IPv6 por las mismas razones.

IPv6 es un nuevo protocolo y es implementado con una nueva seguridad la cual tiene sus defectos. Sin embargo, IPv6 como protocolo resuelve más temas relacionados a la seguridad que IPv4. Por ejemplo, la típica búsqueda de direcciones en una subnet de una red con IPv6 es más difícil, debido a que ahora se tienen  $2^{64}$  posibilidades en las cuales buscar, y es más difícil aún si la dirección la utiliza el nodo sólo temporalmente.

La ausencia de NAT y PAT ayuda en el diseño de políticas de seguridad, detección de fallas y en el desarrollo de servicios de seguridad tal como IPsec. Los protocolos del conjunto de protocolos IPv6 son ahora más seguros, pues utilizan los servicios de seguridad de IPsec.

Después de un período inicial en el que se arreglan los errores en la nueva implementación y de las fallas del nuevo protocolo IPv6, el protocolo IPv6 se volverá mucho más seguro que IPv4. La comunidad deberá haber aprendido de las deficiencias de IPv4 y hacer las mejoras pertinentes en el nuevo

protocolo IPv6, y así con el transcurrir del tiempo, obtener una red más segura con el nuevo protocolo IPv6.

#### **4.1.1 IPsec**

Con el enfoque en que se verá IPsec para IPv6, se pueden distinguir los objetivos o requerimientos de la seguridad:

- **Confidencialidad.** Es la capacidad de transmitir información que puede ser usada o leída únicamente por las partes autorizadas.
- **Integridad.** Es la capacidad de poder detectar si la información no ha sido modificada.
- **Autenticación.** Es la capacidad de poder verificar el proveedor de la información.

IPsec tiene dos modos de encapsulamiento, que son el modo de transporte y el modo túnel. En el modo de transporte, cuando dos nodos establecen una conexión IP segura, ésta se realiza desde el nodo inicial hasta el nodo final sin ningún intermediario. En cambio en el modo túnel cuando los nodos establecen dicha conexión IP segura, ésta se realiza por medio de un servidor seguro VPN (*Virtual Private Network*). Esto quiere decir que el nodo inicial establece una conexión IP segura con el servidor, el nodo inicial encapsula su tráfico hacia el servidor VPN, una vez haya llegado la información encapsulada al servidor VPN, el servidor desencapsula dicho tráfico y lo envía al nodo final. Estos dos modos de encapsulamiento pueden ser combinados de diferentes maneras.

#### **4.1.1.1 Asociaciones de seguridad**

Por cada par de nodos es necesario que estén de acuerdo en cierta información para que puedan utilizar la seguridad de IPv6. Este grupo de información está constituida por: la llave, la autenticación, el algoritmo de encriptación a utilizar y otros parámetros específicos del algoritmo a utilizar, dicho grupo de información constituye un SA (*Security Association*) o una asociación de seguridad entre dos compañeros de comunicación. Dichos SA son unidireccionales y se requiere un SA por cada servicio de seguridad. Debido a los dos tipos de encapsulamiento que existen, es necesario que existan dos tipos de asociaciones de seguridad, los cuales son el de transporte y el de modo túnel. Los servicios SA pueden ser proporcionados para AH o para ESP, pero no para los dos. Se requiere un SA para AH y otro para ESP.

Las SA tienen que ser administradas en dos bases de datos, la primera es la SAD (*Security Association Database*) y la segunda es la SPD (*Security Policy Database*), las cuales son requeridas en cada interface habilitada con seguridad.

#### **4.1.1.2 Cabecera de autenticación AH**

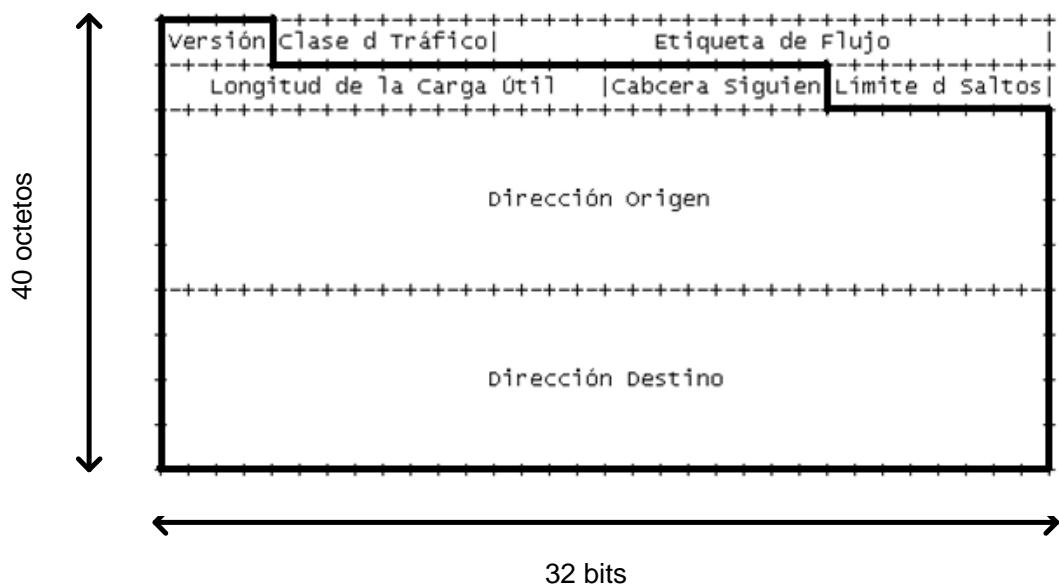
La autenticación por sí sola no proporciona todos los elementos de seguridad necesarios señalados, pero a su vez, no todas las aplicaciones requieren estas características. La cabecera de autenticación AH de IPsec (RFC 2402) provee:

- Integridad a todo el paquete
- Autenticación de la fuente
- Protección de retransmisión



En un paquete IPv6, la cabecera de autenticación provee protección a los campos versión, longitud de carga útil, siguiente cabecera, dirección origen, dirección destino, cabeceras de extensión y a los datos. Además los campos en la cabecera que cambien de valor de una manera impredecible, durante el camino en que viaja hasta llegar a su destino, no puede ser protegido. Es por esto que el campo clase de tráfico no puede ser protegido pues éste puede cambiar su valor por los enrutadores, al igual que el campo de etiqueta de flujo que puede ser cambiado en los diferentes dominios de QoS, y también el campo límite de saltos el cual va disminuyendo de valor en cada enrutador que pasa. Esto se muestra en la figura 53

**Figura 53. Campos del datagrama IP protegidos por AH de IPsec**

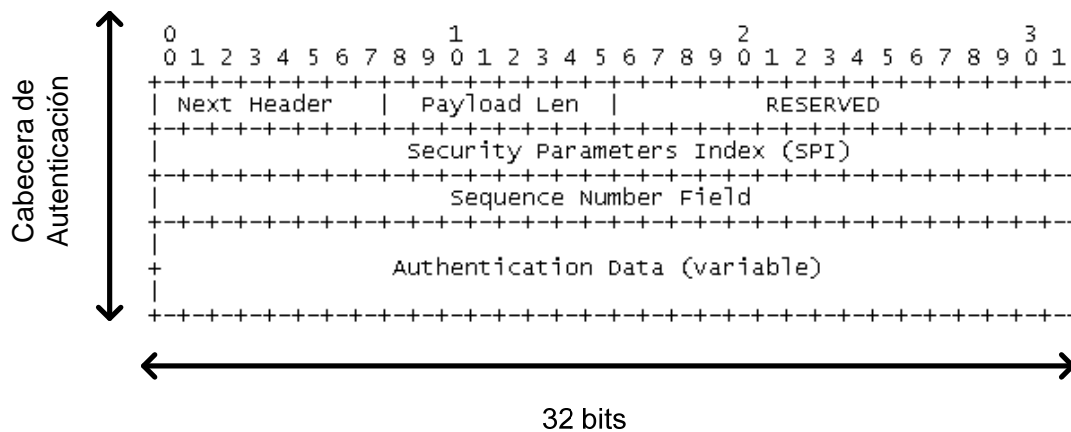


La protección se hace calculando una comprobación de suma criptográfica en los campos protegidos. Esta comprobación de suma, así como las SA, son almacenadas en la cabecera de extensión AH y se identifican con un valor de 51 en el campo siguiente cabecera.

AH puede ser aplicado solo, puede ser aplicado en combinación con el encapsulamiento seguro de carga útil IP (ESP), o aplicado en una modalidad túnel.

La cabecera del protocolo IPv6 que precede inmediatamente a la cabecera AH tendrá un valor de 51 en su campo siguiente cabecera para IPv6 o en el campo protocolo para IPv4. El formato de la cabecera AH se muestra en la figura 54.

**Figura 54. Formato de cabecera AH**



Fuente: RFC 2402, página 2.

El campo siguiente cabecera es un campo de 8 bits que identifica el campo de carga útil que le sigue a AH. Si no existe ninguna otra extensión de cabecera, en el modo transporte usualmente es el número del protocolo de transporte, en el modo túnel es usualmente el número del protocolo IP, que para el caso de IPv6 es 41.

El campo longitud de carga útil es un campo que especifica únicamente la longitud de la cabecera de autenticación.

El campo índice de parámetros de seguridad (SPI), es un campo que en combinación con la dirección destino, identifica de forma exclusiva la asociación de seguridad SA.

El campo número de secuencia, especifica un contador incremental que se utiliza en el servicio anti-replay.

El campo de autenticación de datos, es un campo de longitud variable que contiene el valor de verificación de integridad (ICV) para el paquete. El campo debe de ser un múltiplo entero de 32.

#### **4.1.1.3 Cabecera ESP**

La cabecera ESP (*Encapsulating Security Payload*) o encapsulamiento de seguridad de carga útil está diseñada para proporcionar un conjunto de servicios de seguridad en IPv6 como:

- Confidencialidad
- Integridad en la parte interior del paquete
- Autenticación de la fuente
- Protección anti-replay

El conjunto de servicios proporcionados depende de las opciones seleccionadas al momento del establecimiento de la asociación de seguridad SA y de donde esté localizada la implementación. ESP no protege el paquete entero.

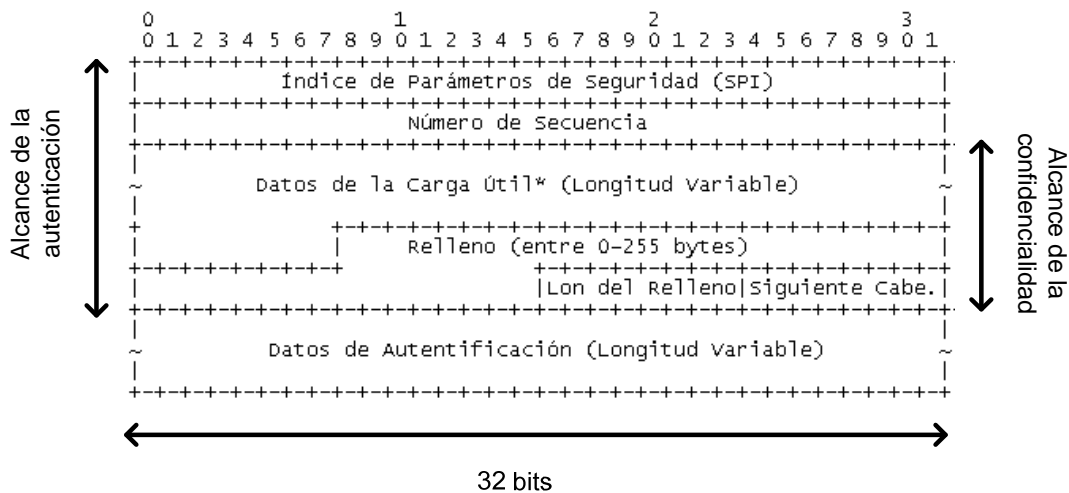
Comparado con AH, ESP agrega la confidencialidad por medio de la encriptación, pero a cambio tiene una limitada protección de integridad pues sólo

la aplica a la carga útil. Una extensión de cabecera ESP está identificada por el valor 50 en el campo siguiente cabecera.

Ninguno de los campos de la cabecera IPv6 está protegido, únicamente el contenido de la carga útil está protegida, incluyendo la cabecera del protocolo de transporte. Si la confidencialidad de ESP se está utilizando, entonces la carga útil es encriptada.

La cabecera ESP se inserta antes que la cabecera IP y después que la cabecera de protocolo de capa superior (en modo transporte) o después de una cabecera IP encapsulada (en modo túnel). El formato de la cabecera ESP se muestra en la figura 55.

**Figura 55. Formato de la cabecera ESP**



Fuente: RFC 2406, página 3.

El campo SPI es un valor arbitrario de 32 bits que, conjuntamente con la dirección destino y el protocolo de seguridad ESP, identifican unívocamente a la asociación de seguridad SA para el datagrama. El conjunto de valores que

puede tomar este campo, que va de 1 a 255, actualmente está reservado por la IANA.

El campo número de secuencia especifica un contador incremental que se utiliza en el servicio anti-replay.

El campo datos de carga útil es un campo de longitud variable que contiene los datos de carga útil del paquete original encriptados.

El campo de relleno es usado para sincronizarse con los tamaños específicos requeridos por los criptoalgoritmos, y existen varios factores que motivan el uso del campo relleno que quedan descritos en el RFC 2406.

El campo longitud del relleno indica el número de bytes de relleno inmediatamente precedentes a este campo. Su rango de valores es de 0 a 255 bytes. Este campo es obligatorio.

El campo siguiente cabecera es un campo de 8 bits que identifica el tipo de datos contenidos en el campo de datos de carga útil. Si no está presente ninguna otra cabecera de extensión, en el modo transporte usualmente se utiliza el número del protocolo de transporte, en el modo túnel se utiliza usualmente el número de protocolo IP (41 para IPv6). Los demás valores de este campo están definidos en el más reciente RFC de "Números asignados" de la IANA.

El campo de datos de autenticación es un campo de longitud variable que contiene el valor de ICV (*Integrity Check Value*) calculado sobre el paquete ESP menos los datos de autenticación. La longitud de este campo queda especificada por la función de autenticación seleccionada. Este campo es

opcional, y se incluye únicamente si el servicio de autenticación se ha seleccionado para la SA que se está tratando.

## **4.2 Mecanismos de migración a IPv6**

IPv6 ha sido diseñado de tal forma que se facilite la migración y la coexistencia con IPv4. Dicha coexistencia con IPv4 puede tardar algunos años, motivo por el cual se han desarrollado varios mecanismos de transición. Existen tres principales categorías de mecanismos de transición:

- Doble pila
- Túnel
- Traducción IPv4 a IPv6

Estos mecanismos de transición pueden ser utilizados solos o en combinación. La migración a IPv6 puede ser realizada paso a paso, comenzando con un nodo o con una subred. También puede darse el caso en que la red sea migrada a IPv6, mientras que nuestro proveedor de servicios (ISP) siga utilizando IPv4 o viceversa.

En este contexto de migración a IPv6, surgen nuevos términos con los cuales se designa a ciertos tipos de nodos, los cuales son:

- Nodo IPv4 únicamente, el cual puede ser un host o un enrutador que implementen únicamente IPv4.
- Nodo IPv6/IPv4, el cual es un host o enrutador que implementan los dos protocolos IPv4 e IPv6.
- Nodo IPv6 únicamente, el cual puede ser un host o un enrutador que implemente únicamente IPv6.

- Nodo IPv6, el cual puede ser un host o enrutador que implemente IPv6. Los nodos IPv6/IPv4 y nodos IPv6 únicamente son nodos IPv6.
- Nodo IPv4, el cual puede ser un host o enrutador que implemente IPv4. Los nodos IPv6/IPv4 y nodos IPv4 únicamente son nodos IPv4.

#### 4.2.1 Doble pila

Este tipo de mecanismo es aquel en el que se tendrá un soporte completo en los nodos así como en los enrutadores para los dos protocolos IPv4 e IPv6. A este tipo de nodo se les denomina nodos IPv6/IPv4, y tienen la habilidad de enviar y recibir los dos tipos de paquetes IPv4 e IPv6, lo cual les permite interoperar directamente con nodos IPv4 usando paquetes IPv4, y además interoperar con nodos IPv6 usando paquetes IPv6. Una pila que ha sido habilitada, tiene una dirección IP asignada, de aquí que un nodo IPv6/IPv4 puede operar en tres modos distintos:

- Con la pila IPv4 habilitada pero la pila IPv6 deshabilitada
- Con la pila IPv6 habilitada pero la pila IPv4 deshabilitada
- Con las dos pilas habilitadas

Dado que los nodos soportan ambos protocolos, dichos nodos adquieren sus direcciones con sus propios métodos, por ejemplo para obtener su dirección IPv4 utiliza DHCP, y el mismo nodo para obtener su dirección IPv6 utiliza DHCPv6.

El DNS (*Domain Name Server*) es utilizado en los dos protocolos para resolver nombres y direcciones IP. Un nodo IPv6/IPv4 necesita un DNS que sea capaz de resolver los dos tipos de registros de direcciones. El registro DNS "A" es usado para resolver direcciones IPv4 y el registro DNS "AAAA" o "A6" es

usado para resolver direcciones IPv6. Si el host que se está resolviendo es de doble pila, entonces el DNS debe devolver los dos tipos de direcciones IP

Una red de doble pila es una infraestructura en la cual la transmisión de ambos protocolos IPv4 e IPv6 está habilitada en los enrutadores. La desventaja es que se deben de tener tablas de enrutamiento para ambos protocolos, y además soporte para ambos protocolos.

#### **4.2.2 Túneles IPv6 sobre IPv4**

Los túneles son una manera de utilizar la infraestructura de enrutamiento IPv4 existente para llevar el tráfico IPv6, hasta el momento en que se cuente con toda la infraestructura IPv6, o sea hasta que toda la red se haya migrado a IPv6.

Los túneles pueden ser usados para llevar tráfico IPv6 encapsulándolo en paquetes IPv4 y tunelizándolo a través de toda la infraestructura de enrutamiento IPv4.

Un túnel tiene dos puntos finales, el primero es el punto de entrada y el segundo es el punto de salida. El túnel puede ser implementado en diferentes maneras:

- Enrutador a enrutador. Los enrutadores IPv6/IPv4 interconectados por una infraestructura IPv4 pueden tunelizar paquetes IPv6 entre ellos.
- Host a enrutador: Los host IPv6/IPv4 pueden tunelizar paquetes IPv6 a un enrutador IPv6/IPv4 intermediario que se alcanza por medio de una infraestructura IPv4.
- Host a host. Los host IPv6/IPv4 que están conectados por una infraestructura IPv4 pueden tunelizar paquetes IPv6 entre ellos mismos.



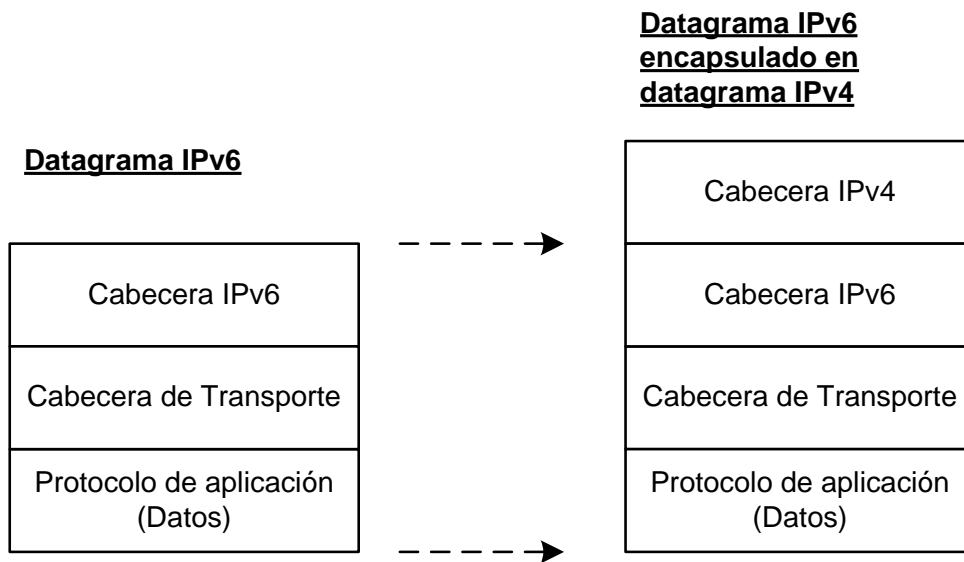
- Enrutador a host. Los enrutadores IPv6/IPv4 pueden tunelizar hacia sus destinos finales que son host IPv6/IPv4.

#### 4.2.2.1 Encapsulamiento

El encapsulamiento de datagramas IPv6 sobre una red IPv4 usa el número de protocolo IPv4 41. El nodo encapsulado puede ser de un host o de un enrutador y el desencapsulado puede ser también cualquiera de los dos.

El datagrama IPv6 es puesto dentro de la carga útil de un datagrama IPv4, tal y como se muestra en la figura 56.

**Figura 56. Encapsulamiento de un datagrama IPv6**



La dirección IPv4 origen y destino del datagrama IPv4 son las direcciones del nodo encapsulado y desencapsulado, las cuales pueden ser o no las direcciones IPv6 origen y destino del datagrama IPv6.

Los pasos del encapsulamiento de un paquete IPv6 son los siguientes:

- El punto de entrada del túnel (el encapsulador) decrementa el campo IPv6, límite de saltos, en una unidad, encapsula el paquete IPv6 en la cabecera IPv4, y transmite el paquete encapsulado a través del túnel. Si fuera necesario el paquete IPv4 es fragmentado.
- El punto de salida del túnel (el desencapsulador) desencapsula el paquete. Si el paquete fue fragmentado, lo reensambla. Luego el punto de salida remueve la cabecera IPv4 y procesa el paquete IPv6 a su destino original.

#### **4.2.2.2 Túnel automático**

Los túneles automáticos permiten a los nodos IPv6/IPv4 comunicarse por medio de la infraestructura IPv4 sin la necesidad de una pre configuración del túnel. La dirección del punto final del túnel está determinado por la dirección compatible IPv4 destino. Este tipo de dirección IPv6 es asignada exclusivamente a los nodos que utilizan túneles automáticos.

Una dirección IPv4 10.12.83.119, tiene como dirección IPv4 compatible ::10.12.83.119, dirección IPv6 en la cual lo que se ha hecho es agregar un prefijo de 96 bits en el cual todos los bits son ceros. La interface a la cual la dirección IPv4 compatible está asignada es llamada comúnmente pseudointerface. Mientras que la dirección IPv4 utilizada no sea una dirección privada, la dirección IPv4 compatible será globalmente única. El túnel automático es creado con la extracción de la dirección IPv4 de la parte baja de la dirección IPv4 compatible.

Una tabla especial de enrutamiento puede ser utilizada para dirigir los paquetes a través del túnel. La ruta será una simple entrada de un prefijo de

ceros con una máscara de 96 bits. Todos los paquetes con una dirección IPv4 compatible como dirección IPv6 destino coincidirán con el prefijo y serán enviados por el túnel automático.

#### **4.2.2.3 Túnel manual**

Los túneles manuales o estáticos requieren que sean configurados en ambos puntos finales, las direcciones origen y destino IPv4 e IPv6, además que los nodos de los puntos finales deben de tener doble pila.

Los túneles estáticos tienen algunos requerimientos. El primer requerimiento es que los dos enrutadores deben de ser doble pila. El segundo requerimiento es que el enrutador de entrada debe de contar con una dirección IPv4 con la cual pueda alcanzar al enrutador de salida y viceversa.

Pero los túneles manuales tienen sus desventajas, una de ellas es que si son varios túneles los que hay que configurar, este trabajo puede ser pesado. Además si las direcciones IP están cambiando para varios túneles el trabajo también se convierte en pesado.

Este tipo de túnel puede ser utilizado cuando se necesitan sólo pocos túneles y cuando no está presente el NAT de IPv4.

#### **4.2.2.4 6to4**

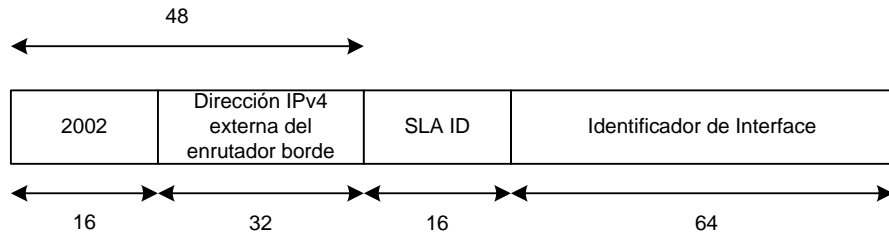
6to4 es un mecanismo (RFC 3056) para que los sitios IPv6 puedan comunicarse entre sí, utilizando la red IPv4, sin la necesidad de contar con un túnel explícito. En este mecanismo surgen nuevas definiciones:

- Pseudo interface 6to4. Es el punto lógicamente equivalente a una interface IPv6 donde ocurre el encapsulamiento 6to4 de los paquetes IPv6 dentro de paquetes IPv4.
- Prefijo 6to4. Es un prefijo propio de 6to4 construido con las características especificadas en el RFC 3056
- Dirección 6to4. Es una dirección IPv6 construida utilizando el prefijo 6to4.
- Dirección IPv6 nativa. Es una dirección IPv6 construida utilizando cualquier otro prefijo que no sea el de 6to4.
- Enrutador 6to4 o de borde. Es un enrutador que soporta las pseudo interfaces 6to4.
- Host 6to4. Es un host IPv6 que debe de tener por lo menos una dirección 6to4.
- Sitio 6to4. Es un sitio en el cual internamente se está corriendo IPv6 usando direcciones 6to4.
- Enrutador relay. Este es un enrutador configurado para soportar rutas con tráfico de direcciones IPv6 nativa y direcciones 6to4.

6to4 es un mecanismo de transición temporal que se utilizará durante el período de tiempo en que coexistan los dos protocolos IPv4 e Ipv6, no será una solución permanente.

La dirección 6to4 está construida en base al prefijo 6to4 2002::/16 seguido por los 32 bits de la dirección IPv4 externa del enrutador de borde del sitio, dando como resultado un prefijo de /48 para el sitio, tal y como se muestra en la figura 57.

**Figura 57. Estructura de la dirección 6to4**

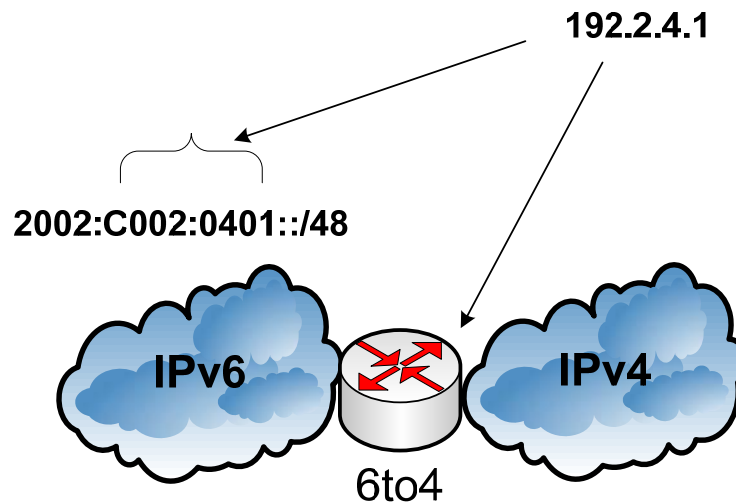


El SLA ID no es más que el identificador de agregación de sitio (*Site Level Aggregation Identifier*). Este es un campo de 16 bits dentro de la dirección global unicast que utiliza una organización para identificar sus subredes dentro de su red. El SLA ID más el identificador de interface dejan 80 bits de espacio de direccionamiento para las redes internas, lo cual es una gran cantidad de espacio de direccionamiento.

La dirección IPv4 externa del enrutador no debe de ser una dirección privada. Además el mecanismo 6to4 necesariamente debe ser implementado sólo en enrutadores de borde. Los hosts dentro del sitio IPv6 no necesitan soportar 6to4.

Por ejemplo, si el enrutador de borde tiene una dirección IPv4 externa 192.2.4.1, el sitio IPv6 detrás de este enrutador usa la dirección 2002:C002:0401::/48 para direccionar a toda la red. Este ejemplo se ilustra en la figura 58.

**Figura 58. Esquema del mecanismo 6to4**



Si los nodos desean comunicarse con otros nodos IPv6 que pertenezcan a redes IPv6 remotas, se necesita un enrutador 6to4 relay. El enrutador relay, como se mencionó, es un enrutador que está configurado para IPv6 y para 6to4, dicho enrutador conecta la red 6to4 a una red IPv6 nativa. Para habilitar 6to4 relay, el enrutador 6to4 relay es un enrutador 6to4 con una ruta por defecto hacia Internet IPv6. Un sitio 6to4 que está utilizando 6to4 relay, instala una ruta IPv6 default en el enrutador 6to4 de borde, apuntando a la dirección 6to4 a la cual se redirige el tráfico. Dichos enrutadores 6to4 relay no requieren algunas características específicas, sino solamente necesitan una ruta estática como entrada.

Un mecanismo adicional para descubrir automáticamente 6to4 relay, es utilizando direcciones IPv4 anycast. La dirección IPv4 anycast utilizada y reservada para este propósito es la dirección 192.88.99.1. 6to4 relay es configurado con esta dirección como dirección secundaria y la infraestructura de enrutamiento IPv4 en la red es configurado para encaminar los paquetes a la

dirección IPv4 especial. Esta dirección anycast provee, además de brindar un mecanismo de descubrir 6to4 relay automáticamente, redundancia y alcance óptimo de la red.

El anuncio del prefijo anycast 6to4 puede hacerse en IGP o en BGP. Sin embargo en cada y más en especial en BGP, se tiene que tener el cuidado que dicho anuncio no vaya más allá de la red a la que se quiere anunciar.

6to4 es utilizado usualmente en redes pequeñas donde no haya necesidad de utilizar NAT en el trayecto, pues 6to4 no puede atravesar NATs. Otra limitación de 6to4 es su vulnerabilidad con respecto al enrutador de borde, pues todo el tráfico 6to4 saldrá únicamente a través de éste, y si este enrutador queda inactivo, toda la red también lo estará.

#### **4.2.2.5 ISATAP**

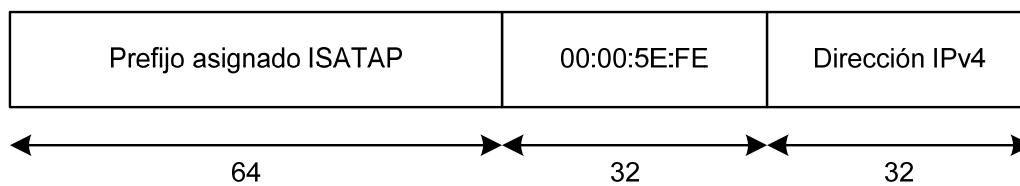
*Intra Site Automatic Tunnel Addressing Protocol* (ISATAP) es un mecanismo que automatiza la creación de túneles de nodos a enrutadores y de nodos a nodos dentro de un sitio. Este mecanismo es diseñado para proveer conectividad IPv6 entre nodos IPv6 en una red que internamente en su mayoría está basado en IPv4 y que no cuenta con un enrutador IPv6. Únicamente si dichos nodos necesitan comunicarse con nodos IPv6 en Internet, entonces sí es necesario la configuración de un enrutador de borde.

ISATAP permite la creación automática de túneles inclusive si se están utilizando direcciones IPv4 privadas o si se está haciendo uso de NAT.

ISATAP aloja la dirección IPv4 del nodo en los últimos 32 bits del identificador de interface de la dirección IPv6. Los primeros 32 bits del

identificador de interface tienen un valor fijo y reservado por la IANA el cual es 00:00:5E:FE los cuales definen ISATAP. La figura 59 muestra el formato de una dirección ISATAP.

**Figura 59. Formato de la dirección ISATAP**



El prefijo de 64 bits puede ser enlace-local, sitio-local, prefijo 6to4, o pertenecer al rango unicast global. El identificador de interface utiliza el IANA OUI 00:00:5E. El siguiente byte es un campo de tipo, el cual tiene un valor de FE que indica que dicha dirección contiene una dirección IPv4 alojada.

Algunos de los requerimientos es que todos los nodos dentro del sitio deben de soportar doble pila, además todos los nodos deben de soportar ISATAP para poder comunicarse y también se necesita un enrutador ISATAP el cual debe quedar configurado como ruta por defecto en todos los nodos dentro del sitio.

ISATAP puede ser utilizado en empresas pero no es recomendado para proveedores o ISP, ni para redes de casa. Además ISATAP no puede atravesar NATs.



#### 4.2.2.6 TSP negociador de túneles

Tunnel bróker o negociador de túneles es un mecanismo cuya idea es dar un enfoque alternativo basado en la disposición de servidores dedicados, llamados Tunnel brokers, los cuales gestionan las requisiciones de túneles que vienen de los usuarios. Se espera que este enfoque pueda estimular el desarrollo y crecimiento de IPv6 .

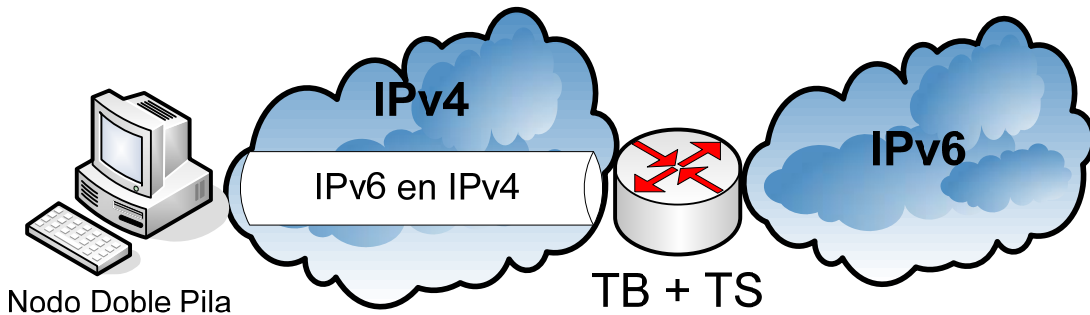
El mecanismo asignado de túneles encaja muy bien en el marco de sitios aislados IPv6, y nodos IPv6 aislados en Internet IPv4, que desean un fácil acceso a la red existente IPv6.

TSP (*Tunnel Setup Protocol*) o protocolo de configuración de túnel, fue diseñado para automatizar el proceso de establecimiento de túneles IPv6 en IPv4, para poder proveer un acceso transparente a IPv6. Es un protocolo de señalización entre el cliente y el corredor, donde el cliente hace el requerimiento del túnel y el corredor envía la información acerca del túnel asignado.

El mecanismo tunnel broker puede ser visto como un ISP de IPv6 virtual, proveyendo conectividad IPv6 a los usuarios que ya están conectados a Internet IPv4. Actualmente se cuenta con una lista de corredores de túneles que están disponibles para prestar este servicio, los cuales se pueden encontrar en la página [www.ipv6.org](http://www.ipv6.org), y sólo basta con escoger el más cercano o el más barato.

El funcionamiento del mecanismo corredor de túneles, está basado en el conjunto de elementos funcionales representados en la figura 60.

**Figura 60. Modelo del mecanismo Tunnel broker**



TB (*Tunnel Broker*) es el lugar donde los usuarios se conectan, por medio de los protocolos de transporte TCP o UDP, para registrar y activar los túneles. Los TB gestionan la creación, modificación y supresión a favor del usuario. Además los TB también pueden registrar la dirección IPv6 y el nombre en el DNS del usuario. Al TB se le debe de poder direccionar en IPv4 y como opción en IPv6.

TS (*Tunnel Server*) es un enrutador de doble pila, conectado al Internet global. Tras la recepción de una orden de configuración procedente del TB, el TS crea, modifica y borra del lado del servidor los túneles. Además también mantiene las estadísticas de uso de cada uno de cada túnel activo.

El usuario del servicio del TB es un nodo (host o enrutador) IPv6 de doble pila conectado al Internet IPv4. El usuario debe de realizar una pre-autorización y autenticación para poder hacer uso de los servicios, y una vez que se le haya dado la autorización, el usuario debe de proveer como mínimo la siguiente información:

- La dirección IPv4 del lado del cliente en el túnel.

- El nombre a utilizarse para el registro en el DNS de la dirección IPv6 global.
- La función del cliente, la cual puede ser la de host o la de enrutador.

Entonces ya con la anterior información el TB maneja el requerimiento del cliente como sigue:

- Primero designa un TS al usuario, el cual va a ser utilizado como el punto final actual del túnel del lado de la red.
- Elige el prefijo IPv6 que va a utilizar el cliente, el cual puede ir de 0 a 128, y los más comunes para un prefijo de sitio es 48, para un prefijo de subred es 64 y para prefijo de host es 128.
- Fija un tiempo de vida para el túnel.
- Automáticamente registra en el DNS la dirección IPv6 global asignada al punto final del túnel.
- Se configura todo lo necesario del lado del servidor del túnel.
- Se le notifica al cliente toda la información de la configuración, incluyendo los parámetros del túnel y los nombres del DNS.

Una vez se haya realizado lo anterior, el túnel IPv6 sobre IPv4 que existe entre el cliente y el TS elegido está activado y funcionando.

Algunas de las limitaciones del mecanismo TSP TB es la distancia entre el cliente TSP y el TS. Otra limitante es que este mecanismo no funciona si el cliente está utilizando una dirección privada IPv4 detrás de un NAT.

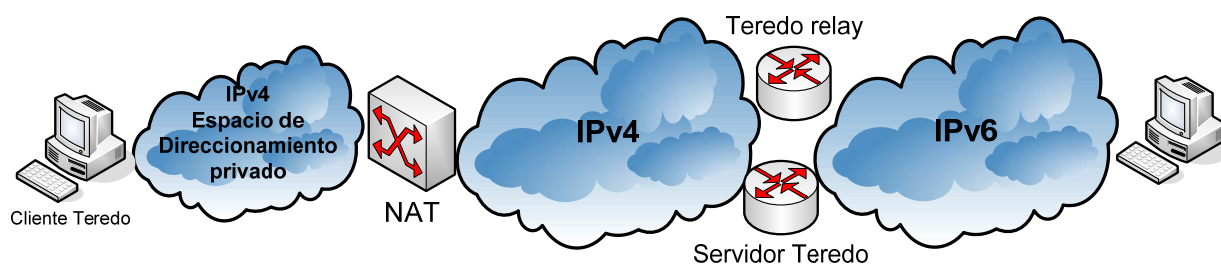
#### 4.2.2.7 Teredo

El mecanismo Teredo (RFC 4380) habilita, en los nodos que están localizados detrás de NATs, un túnel IPv6 sobre IPv4 para garantizar la conectividad IPv6 utilizando el protocolo de transporte UDP. Para ello Teredo hace uso de servidores Teredo así como de Teredo relays.

Un servidor Teredo es un nodo que tiene acceso a Internet IPv4 a través de una tabla de enrutamiento global y que ayuda a proveer conectividad IPv6 a los clientes Teredo. El Teredo relay es un enrutador que puede recibir el tráfico destinado a un cliente Teredo y reenviarlo utilizando los servicios Teredo.

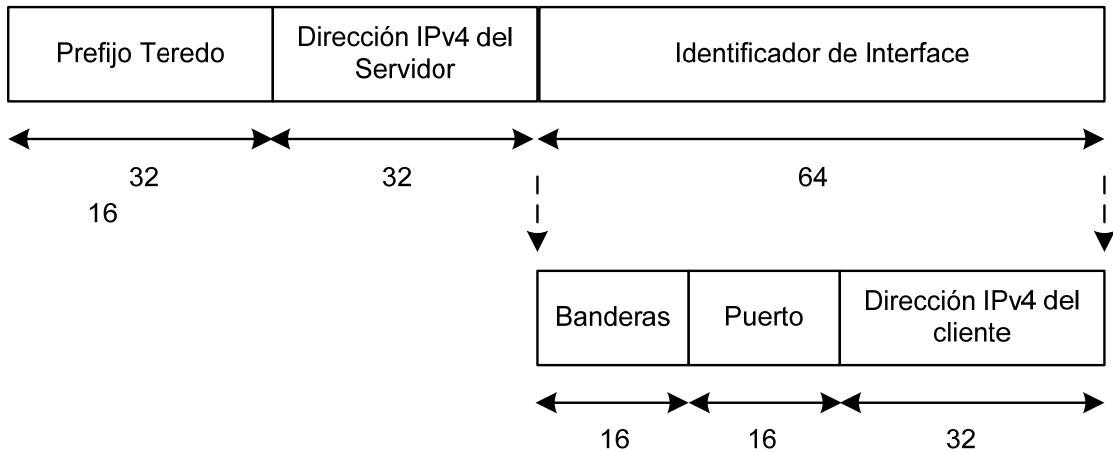
Un cliente Teredo recibe la dirección IPv6 de un servidor Teredo y atraviesa NAT IPv4 usando encapsulamiento IPv6 sobre UDP-IPv4. Los componentes del mecanismo Teredo se ilustran en la figura 61.

**Figura 61. Modelo del mecanismo Teredo**



Tal y como 6to4, Teredo utiliza un prefijo especial para proveer la dirección IPv6 a los nodos. La dirección Teredo está compuesta de cinco componentes los cuales se ilustran en la figura 62.

**Figura 62. Formato de la dirección Teredo**



El campo prefijo Teredo, es un prefijo de 32 bits asignado por la IANA. El siguiente campo indica la dirección IPv4 del servidor Teredo. El campo identificador de interface está compuesto por tres sub campos que son el de bandera, el de puerto, y la dirección IPv4 del cliente. El sub campo de banderas es un conjunto de 16 bits que documentan el tipo de dirección y el tipo de NAT (existen 2 tipos, el tipo cono y el tipo no cono). El sub campo puerto, es un campo de 16 bits que indica el número de puerto del NAT del cliente. El último sub campo indica la dirección IPv4 del cliente.

Para poder desplegar Teredo, todos los nodos deben de ser doble pila, además de implementar Teredo en cada uno. Otro requerimiento es que no debe de existir NAT simétrico entre el nodo Teredo y el servidor Teredo. Además también se requiere que el servidor Teredo sea configurado estáticamente en todos los clientes Teredo.

Las aplicaciones del mecanismo Teredo son restringidas, debido a varias de sus limitantes. Este mecanismo funciona para nodos IPv6 aislados que

están detrás de ciertos tipos de NATs donde no es necesario una dirección IPv6 estable.

#### **4.2.2.8 GRE soportando IPv6**

El tráfico IPv6 puede ser transportado a través de los túneles GRE (*Generic Routing Encapsulation*) que se utilizan en IPv4. Este tipo de túnel GRE soportando IPv6, son enlaces entre dos puntos, con un túnel separado para cada enlace. Los túneles no están restringidos a un pasajero en específico o a un protocolo de transporte, pero en este caso tiene como protocolo pasajero a IPv6 y a GRE como el protocolo transportador.

El uso principal de los túneles GRE es para realizar conexiones estables que requieren una regular comunicación segura entre dos enrutadores. Los enrutadores deben ser doble pila.

GRE posee un campo que identifica el protocolo pasajero. Los tipos de pasajeros que pueden ir son IPv6 o IS-IS, lo cual habilita que tanto IPv6 como IS-IS viajen en el mismo túnel.

### **4.3 Configuraciones necesarias para la migración a IPv6**

La migración de las redes IPv4 al nuevo protocolo IPv6, incluye muchos aspectos de planificación, configuración, medición y corrección. De los anteriores la configuración es una de las más importantes y de las que trataremos a profundidad en este trabajo.

La configuración necesaria, ya sea para migrar hacia IPv6 o para crear una red IPv6 nativa, conlleva muchos aspectos que serán tratados. Pero

además dicha configuración se vuelve aún más compleja pues en la actualidad en los mercados guatemaltecos, ya sea en las redes de los proveedores de servicios (ISP) más importantes que existen en Guatemala, o en las redes de las empresas, o en la red de nuestra casa, se cuenta con una gran gama de proveedores o *vendors* de equipos para redes que utilizamos para poder conectarnos a Internet.

Este trabajo de investigación se concentrará en la configuración de los equipos de marcas más utilizadas y comunes del mercado guatemalteco que son Cisco y Windows.

#### **4.3.1 Configuración de interfaces y avisos de enrutadores**

En la siguiente sección se describirá como se habilita IPv6, la configuración de una interface y la configuración de los avisos de los enrutadores para Windows XP y para Cisco.

Bajo la plataforma Windows XP, para poder habilitar IPv6, dado que cuando se instala Windows XP no se habilita de manera predeterminada IPv6, es necesario ejecutar el siguiente comando:

**>netsh interface ipv6 install**

Para la configuración manual de una interface en Windows XP, en la cual se asigna una dirección a una interface, se debe ejecutar el siguiente comando:

**>netsh interface ipv6 address "nombre de la interface" 2EEF:B001:0:1:A**

Para la parte de solucionar problemas o troubleshooting, los siguientes comandos pueden ser útiles:

Para desplegar direcciones IPv6 en interfaces:

**>netsh interface ipv6 show address**

Para desplegar las direcciones IPv4 e IPv6, la configuración del DNS y la ruta por defecto de todas las interfaces:

**>ipconfig**

Para hacer un ping a una dirección IPv6 en específico:

**>ping 2EEF:B001:0:1:A**

Para forzar el uso de IPv6, se ejecuta el comando:

**>ping -6 www.ipv6.org**

Bajo la plataforma del proveedor Cisco, se tienen comandos para habilitar IPv6, configurar una interface y configurar los anuncios de los enrutadores para el IOS 12.2.(13) en específico.

Para habilitar IPv6 en el modo de configuración global, se deben de ejecutar los siguientes comandos:

**>configure terminal**

**>ipv6 unicast-routing**

Para configurar una interface, en el modo de configuración de interface se deben de ejecutar los siguientes comandos:

**>configure terminal**

**>interface Ethernet0**

**(config-if)>ipv6 address 3FFE:B00:0:1::1/64**



También se pueden configurar dirección del tipo enlace-local y para ello se debe de ejecutar como sigue:

```
(config-if)>ipv6 address 3FFE:B00:0:1::1/64 link-local
```

Dado que IPv6 soporta múltiples direcciones en la misma interface, en IPv6 no es necesario agregar el término “secondary” que se necesitaba en IPv4.

La configuración de los anuncios de los enrutadores se debe de realizar en cada una de las interfaces IPv6 habilitadas. Para ello es necesario ejecutar los siguientes comandos:

```
>configure terminal
```

```
>interface Ethernet0
```

```
(config-if)>ipv6 nd prefix-advertisement address 3FFE:B00:0:1::1/64
```

Para la parte de troubleshooting en Cisco, se pueden utilizar los siguientes comandos:

Verificar la dirección IPv6 en una interface:

```
>show ipv6 interface ethernet0
```

Hacer un ping a la dirección del mismo host de donde se está emitiendo el ping:

```
>ping ipv6::1
```

Para desplegar un sumario del tráfico IPv6 que ha cursado:

```
>show ipv6 traffic
```

Para habilitar el debug de los paquetes del descubrimiento de vecinos, se ejecutar el comando:

```
>debug ipv6 nd
```

### 4.3.2 Gestión de vecinos en host y enrutadores

En esta sección se verá los comandos necesarios para la gestión de las vecindades en un enlace específico, tanto para Windows XP como para Cisco.

En el caso de la plataforma Windows, el comando para mostrar el cache de los vecinos es:

**>netsh interface show neighbors**

Para establecer el MTU en una interface en específico, se debe ejecutar:

**>netsh interface ipv6 set interface interface="nombre de la interface" mtu=1480**

Para el caso del proveedor Cisco, el comando para mostrar las vecindades es:

**>show ipv6 neighbors**

En el anterior comando, el nombre de una interface o la dirección de la misma, se pudo haber especificado después de "neighbors" para restringir el despliegue de la información de vecindades.

Para limpiar el cache de vecindades, se ejecuta el comando:

**>clear ipv6 neighbors**

Para agregar un vecino (EE80::212:BBF:FFEA:0A0A) con una dirección de capa de enlace 01:13:6C:4A:8E:8A en una interface en específico (Ethernet0), los comandos a ejecutarse son:

**>configure terminal**

**>ipv6 neighbor EE80::212:BBF:FFEA:0A0A Ethernet0 01:13:6C:4A:8E:8A**

### **4.3.3 Gestión de mensajes ICMP en host y enrutadores**

En Windows XP, para enviar un ICMP echo request a un nodo, se utiliza el ping, como se había visto, pero si se desea enviar a una dirección enlace-local, el comando a ejecutar debe ser:

**>ping FE80::1%3**

En el cual se envía la dirección de enlace-local, y seguido se añade el símbolo “%” y el índice de la interface al cual el paquete debe ser enviado.

En Cisco, para habilitar un límite para los mensajes ICMP con el objetivo de evitar ataques de “denegación de servicio”, es posible configurar dicho límite con el siguiente comando:

**>configure terminal**

**>ipv6 icmp error-interval 100**

### **4.3.4 Configuración estática de un servidor DNS**

En Windows XP, para configurar la entrada estática de un servidor DNS, se debe de utilizar el siguiente comando:

**>netsh interface ipv6 add dns FFEE:B00:0:1::4**

Por defecto en Windows, si un nombre destino tiene las dos direcciones IPv4 e IPv6 en el servidor DNS, entonces la dirección IPv6 tendrá prioridad sobre la IPv4.

En Cisco, para configurar la entrada estática de un servidor DNS, se debe ejecutar, en el modo de configuración global, el comando:

```
>configure terminal
```

```
>ip name-server FFE0:B00:0:1::4
```

#### **4.3.5 Configuración de enrutamiento**

Anteriormente se había mencionado cada uno de los protocolos de enrutamiento para IPv6. A continuación se abordará a profundidad las configuraciones necesarias en los host y en los enrutadores para poder implementar cada uno de los protocolos de enrutamiento, tanto en Windows XP como en equipos Cisco, tal y como se ha estado analizando.

Como se había mencionado anteriormente la interfaces de los enrutadores pueden tener una configuración automática, la cual está basada en la dirección MAC de la tarjeta de red, pero esto hace que la dirección sea dependiente del hardware, y un reemplazo del hardware dañado ocasiona una nueva auto-configuración, lo cual puede ser algo no tan bueno, dado que la red ya estaba diseñada y desplegada de una cierta manera. Debido a esto, no es tan recomendada la auto-configuración de las interfaces de los enrutadores, y es preferible la configuración de direcciones estáticas en las interfaces de los enrutadores.

#### 4.3.5.1 Rutas estáticas

En Windows XP, para agregar una ruta estática, se debe de usar la sentencia “add route” y especificar el prefijo de la ruta, la interface y el siguiente salto. A continuación se ilustra un ejemplo en el cual se agrega una ruta por defecto en la interface ethernet0 y con la dirección FE80::1 como siguiente salto:

```
>netsh interface ipv6 add route ::/0 ethernet0 nexthop=FE80::1  
publish=yes
```

Para borrar una ruta, se debe de hacer tal y como sigue:

```
>netsh interface ipv6 delete route ::/0 ethernet0
```

En Cisco, las rutas estáticas son configuradas usando el comando “ipv6 route”. En el siguiente ejemplo se configura la ruta estática 4EEF:C00:1:0::/64 dirigida a FE80::2:

```
>configure terminal  
>ipv6 route 4EEF:C00:1:0::/64 FE80::2
```

Para listar las rutas configuradas en un enrutador, se utiliza el comando:

```
>enable  
>show ipv6 route static
```

#### 4.3.5.2 IPv6 forwarding / CEF

En Windows, por defecto IPv6 forwarding está apagado, para habilitarlo, se debe de utilizar la sentencia “set forwarding” en cada interface, tal y como sigue:

**>netsh interface ipv6 set interface ethernet0 forwarding=enabled**

En Cisco, IPv6 forwarding no está explícitamente configurado, un enrutador Cisco se comporta como un host IPv6 y no transmite paquetes IPv6. Para habilitar IPv6 forwarding se debe de utilizar el comando “ipv6 unicast-routing”, tal y como sigue:

**>configure terminal**  
**>ipv6 unicast-routing**

Para habilitar IPv6 *Cisco Express Forwarding* (CEF) se debe de utilizar la sentencia “ipv6 cef”, pero a la vez IPv4 CEF debe habilitarse usando la sentencia “ip cef”. Los paquetes IPv6 con direcciones, origen y destino, globales son cambiadas a CEF. Paquetes IPv6 con direcciones enlace-local no son cambiadas a CEF. Los comandos para habilitar IPv4 e IPv6 CEF son:

**>configure terminal**  
**>ip cef**  
**>ipv6 cef**

Los comandos necesarios para distribuir CEF son:

**>configure terminal**

```
>ip cef distributed
>ipv6 cef distributed
```

#### 4.3.5.3 RIP

En Cisco, para habilitar RIP se debe ejecutar el comando “ipv6 router rip”. Los procesos RIP son definidos con un único nombre. Los anuncios RIP se comienzan a enviar cuando el proceso es añadido a una interface utilizando el comando “ipv6 rip enable” en el modo de configuración de interface. Un ejemplo de la configuración RIP para IPv6 con un proceso llamado R1 que es habilitado en la interface Ethernet0 se muestra a continuación:

```
>configure terminal
>ipv6 router rip R1
>interface ethernet0
(config-if)>ipv6 rip R1 enable
```

Para redistribuir una ruta estática en los anuncios RIP, use la sentencia “redistribute static” bajo el modo de configuración ipv6 router rip, tal y como sigue:

```
>configure terminal
>ipv6 router rip R1
>redistribute static
```

La información de RIP es desplegada por medio del comando:

```
>show ipv6 rip
```

#### 4.3.5.4 OSPF

La mayoría de comandos OSPFv3 son parecidos a los utilizados en OSPF para IPv4. La única diferencia significativa es que OSPFv3 es habilitado en cada interface.

Para empezar a habilitar OSPF, se debe de ingresar la sentencia “ipv6 router ospf”. Con este comando se entra a un sub modo de configuración para agregar otras sentencias de configuración OSPF. Para iniciar el anuncio de OSPF en una interface, se debe de utilizar la sentencia “ipv6 ospf” en el modo de configuración de interface. Estos comandos se ilustran en el siguiente ejemplo:

```
>configure terminal  
>ipv6 router ospf  
>interface Ethernet0  
(config-if)>ipv6 ospf
```

Para redistribuir las rutas BGP en OSPF, se debe utilizar el comando “redistribute bgp” con el número de AS del proceso BGP, tal como sigue:

```
>configure terminal  
>router bgp “número de AS”  
>ipv6 router ospf  
>redistribute bgp “número de AS”
```

La información de OSPF es desplegada por medio del comando “show ipv6 ospf” en el modo privilegiado, tal como sigue:



```
>enable  
>show ipv6 ospf
```

Para reinicializar los cálculos de SPF, se debe utilizar el comando “clear ipv6 ospf force-spf”, tal como sigue:

```
>enable  
>clear ipv6 ospf force-spf
```

#### **4.3.5.5 IS-IS**

Para el caso de IS-IS en Cisco, IS-IS lleva consigo las rutas de IPv4 e IPv6 en el mismo protocolo y en el mismo proceso, por lo que pocos comandos son agregados para IPv6.

La sentencia “address-family ipv6” es usada para habilitar IPv6 en IS-IS. La sentencia “ipv6 router isis” es usada, en el modo de configuración de interface, para habilitar IS-IS en una interface específica. El siguiente ejemplo muestra el proceso IS-IS llamado A1 con la familia de direcciones IPv6 que están asignadas a la interface Ethernet0 cuya dirección es 172.16.1.1 y cuya área es 49.001

```
>configure terminal  
>router isis A1  
>net 49.001.1720.1600.1001.00  
>address-family ipv6  
>interface ethernet0  
(config-if)>ipv6 router isis A1
```

Para redistribuir las rutas BGP en IS-IS, se debe de utilizar la sentencia “redistribute bgp” bajo el modo “address-family ipv6”. Además, siempre bajo esta misma modalidad, para añadir una ruta por defecto en los anuncios IS-IS, se debe de utilizar la sentencia “default-information originate”, tal como se muestra:

```
>configure terminal  
>router isis A1  
>address-family ipv6  
>redistribute bgp 65000  
>default-information originate
```

La información de IS-IS es desplegada por medio del comando “show isis”, tal como sigue:

```
>enable  
>show isis A1
```

#### **4.3.5.6 BGP**

Para habilitar el enrutamiento BGP se debe de utilizar la sentencia “router bgp” seguido por el número de AS. Con esto se logra entrar a un sub modo para configurar parámetros adicionales de BGP.

La configuración de BGP se realiza en dos partes. La primera es establecer la relación de vecindades entre los enrutadores, y la segunda parte se trata de intercambiar las rutas.

La relación de vecindades entre los enrutadores es establecida con la sentencia “neighbor remote-as”. El intercambio de rutas IPv6 es activado con la sentencia “address-family ipv6” usando la sentencia “neighbor activate”.

En el siguiente ejemplo, se configurará BGP para IPv6 con un AS 65001 y con un identificador de enrutador de 192.0.2.1, el cual intercambiará información con su igual que pertenece a otro AS 65002 con una dirección 3FFE:C00:1:1::1. Además bajo la familia de direcciones IPv6, se activará el intercambio de rutas con el vecino y se le anunciará la ruta 3FEE:B00::/24.

```
>configure terminal  
>router bgp 65001  
>bgp router-id 192.0.2.1  
>neighbor 3FFE:C00:1:1::1 remote-as 65002  
>address-family ipv6  
>neighbor 3FFE:C00:1:1::1 activate  
>network 3FEE:B00::/24
```

Cuando se está intercambiando únicamente rutas IPv6 sin rutas IPv4, se debe de utilizar la sentencia “no bgp default ipv4-unicast” bajo el modo de configuración de enrutador, dado que por defecto las rutas IPv4 son intercambiadas.

Para ver detalles del proceso de BGP, en el modo privilegiado se debe de utilizar el comando “show bgp ipv6”.

### 4.3.6 Configuración de túneles

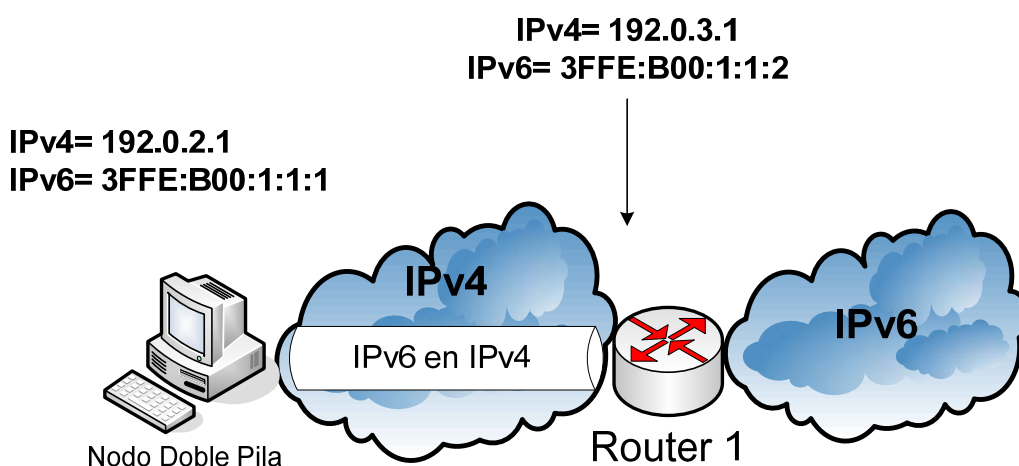
A continuación se describirá cuáles son las configuraciones necesarias para poder hacer uso de los distintos mecanismos de transición vistos anteriormente, tanto en Windows XP como en el proveedor Cisco.

Las configuraciones de los distintos tipos de túneles es una de las últimas configuraciones necesarias que hay que realizar para poder obtener la conectividad a Internet IPv6.

#### 4.3.6.1 Túnel estático

Para ejemplificar la configuración de un túnel estático IPv6 en IPv4, se presenta la figura 63.

Figura 63. Ejemplo de túnel estático



En Windows, una interface túnel siempre es creada por defecto y usualmente es la interface número 2. Para configurar el túnel estático IPv6 en IPv4, se deben de ejecutar los siguientes comandos:

```
>netsh interface ipv6 add route prefix=::/0 interface=2
nextHop=::192.0.3.1 publish=yes
>netsh interface ipv6 add
Address interface=2
Address=3FFE:B00:1:1::1
```

En los enrutadores Cisco, los comandos a ejecutar para poder realizar los túneles estáticos son los siguientes:

```
>configure terminal
>interface tunnel 0
(config-if)>ipv6 address 3FFE:B00:1:1::1/128
(config-if)>tunnel source 192.0.2.1
(config-if)>tunnel destination 192.0.3.1
(config-if)>tunnel mode ipv6ip
```

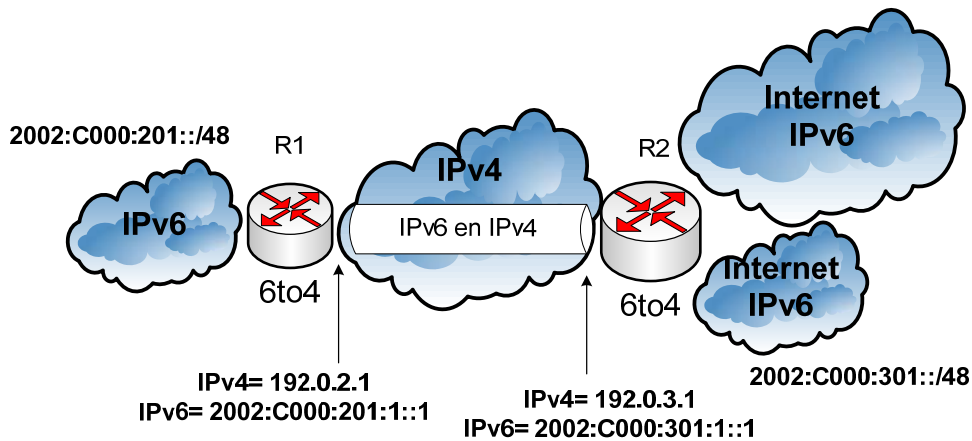
#### 4.3.6.2 6to4

Para ejemplificar la configuración de 6to4, se presenta la figura 64.

En Windows, por defecto se crea una dirección 6to4 para cada una de las direcciones IPv4 públicas asignadas a todas las interfaces. Además también se crea una ruta 2002::/16 para poder reenviar a la pseudo-interface 6to4. Así mismo también se realiza una requisición automática para hallar el enrutador relay. Para establecer un enrutador 6to4 relay manualmente se de ejecutar el comando:

```
>netsh interface ipv6 6to4 set relay 192.0.3.1
```

Figura 64. Ejemplo de 6to4



En Cisco, 6to4 es implementado con un nuevo modo de túnel llamado “ipv6ip 6to4” en el modo de configuración interface túnel. Los comandos a ejecutarse son los siguientes:

```
>configure terminal
>interface tunnel 0
  Ipv6 address 2002:C000:201:1::1/64
  Tunnel source 192.0.2.1
  Tunnel mode ipv6ip 6to4
```

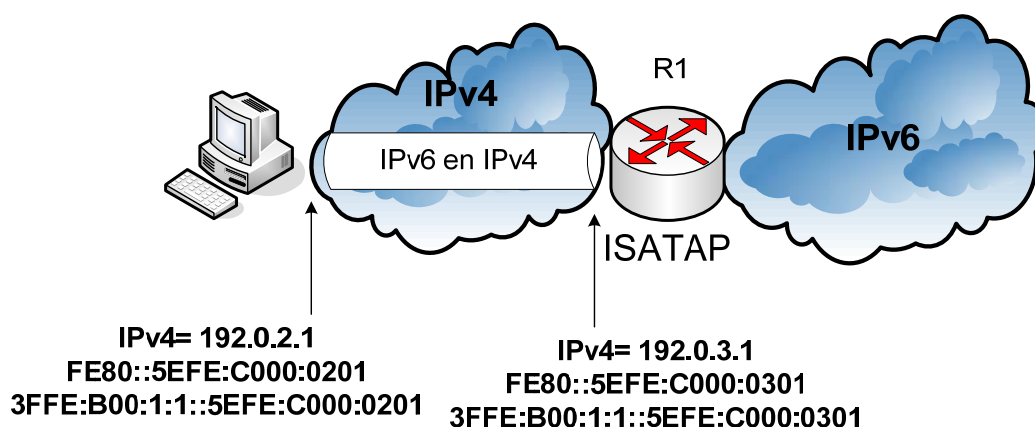
Para poder reenviar los paquetes entrantes 6to4 a través de la interface 6to4, se debe instalar una ruta específica 6to4 hacia la interface 6to4, tal y como se realiza con los siguientes comandos:

```
>configure terminal
>route 2002::/16 tunnel 0
```

### 4.3.6.3 ISATAP

Para ejemplificar la configuración de ISATAP, se presenta la figura 65.

Figura 65. Ejemplo de ISATAP



En Windows, para ISATAP también se crea por defecto una dirección enlace-local para todas las direcciones públicas IPv4 asignadas en todas las interfaces. Además también se hace una requisición automática de DNS para hallar el enrutador ISATAP. Para configurar el enrutador ISATAP manualmente es usado la sentencia “`isatap set router`”, tal y como sigue:

```
>netsh interface ipv6 isatap set router 192.0.3.1
```

En Cisco, ISATAP es implementado en un nuevo modo túnel llamado “`ipv6ip isatap`”, en el modo de configuración interface túnel, tal y como sigue:

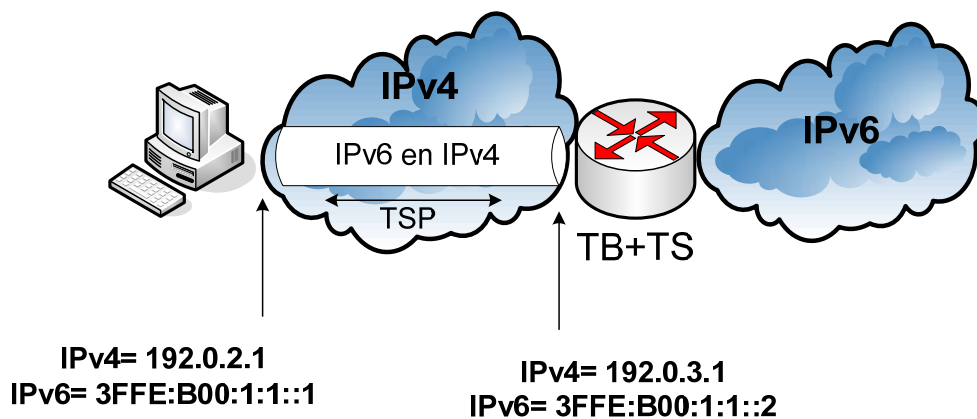
```
>configure terminal  
>interface tunnel 0  
  ipv6 address 3FFE:B00:1:1::/64 eui-64
```

**Tunnel source 192.0.2.1**  
**Tunnel mode ipv6ip isatap**

#### 4.3.6.4 TSP negociador de túneles

Para ejemplificar la configuración de un cliente TSP negociador de túneles, se presenta la figura 66.

**Figura 66. Ejemplo de un cliente TSP tunnel broker**



En Windows una manera de habilitar un cliente TSP tunnel broker es por medio del sitio web <http://www.freeenet6.net>. El cliente TSP tunnel broker usa la interface número 2 para los túneles IPv6 en IPv4. El archivo "tspc.conf" es usado para configurar el cliente. El cliente TSP se activa con la línea de comando "tspc".

En el IOS de Cisco para la configuración del cliente TSP/TB, existe una plantilla o template. El cliente puede ejecutar esta plantilla en cualquier plataforma, ya sea Windows, Linux, o cualquier otra, con sólo especificar "template=cisco". El archivo "tspc.conf" es usado para configurar el cliente.



#### **4.3.6.5 GRE soportando IPv6**

En Cisco, cuando un túnel GRE es configurado, se le asignan direcciones IPv6 al origen y al destino de dicho túnel. La interface túnel puede tener direcciones IPv4 e IPv6 asignadas. El nodo o el enrutador al final del túnel debe ser doble pila. Los comandos utilizados para habilitar el túnel GRE son:

**>enable**

**>configure terminal**

**>interface túnel “número del túnel”**

**>ipv6 address “prefijo-ipv6/longitud-prefijo”**

**>tunnel source “dirección ó interface del origen”**

**>tunnel destination “dirección IPv4 ó nombre del host destino”**

**>tunnel mode “GRE IPv6”**



## CONCLUSIONES

1. Las redes de computadoras, como por ejemplo Internet, hoy en día desempeñan un importante papel en cualquier área o mercado de nuestras sociedades, es por ello que debe contar con una estructura robusta la cual debe de ser mejorada continuamente.
2. Dado al rápido crecimiento de la cantidad demandada de direcciones IP, debido a su vez por el nacimiento de nuevas aplicaciones que utilicen ese tipo de direcciones, se puede observar, con base a modelos dinámicos predictivos desarrollados con series de tiempo, que el agotamiento de dichas direcciones en IPv4 llegará a su límite en aproximadamente algunos años a partir de ahora.
3. Debido al agotamiento de las direcciones IPv4, es de suma importancia que todas las redes sean migradas lo antes posible al nuevo protocolo IPv6, para aprovechar todavía este tiempo que queda como tiempo de transición o tiempo de experimentación para solventar los posibles inconvenientes que puedan darse en la migración.
4. IPv6 es un paso, más bien evolucionario y no revolucionario de IPv4, dado por la IETF, el cual conserva muchas de las bondades de IPv4, pero a la vez mejora las debilidades de IPv4. IPv6 permite direccionar  $2^{128}$  nodos, y lo hace con una arquitectura de direcciones simple y fija, lo cual permite una fácil planificación reduciendo así el manejo de las redes.

5. La seguridad que conlleva el migrar a IPv6, es un aumento en la seguridad a nivel de capa de red, pues IPsec se vuelve obligatorio, lo cual permite crear toda una estructura de seguridad más robusta, y da paso a crear aplicaciones más seguras.
6. Windows y Cisco ya tienen el soporte necesario para poder migrar aquellas redes que cuenten con una estructura desarrollada en dichas plataformas, los comandos necesarios para dicha migración ya fueron creados y lo único que se necesita es una buena planificación para posteriormente poner en marcha la migración a IPv6 para poder aprovechar las bondades de este nuevo protocolo.

## RECOMENDACIONES

1. Actualmente un buen porcentaje de redes están todavía trabajando con el protocolo IPv4, y sólo un pequeño porcentaje ya lo comienza a hacer con el nuevo protocolo IPv6. Debido a esto, se considera que éste es un buen momento de experimentación para comenzar a hacer las pruebas de migración hacia el nuevo protocolo IPv6, así como de comenzar a familiarizarse con las características propias de IPv6 y con ello poder realizar una buena planificación de migración.
2. Uno de los primeros pasos experimentales de migración puede ser comenzar a migrar pequeñas sub-redes experimentales que formen parte de nuestra red, y que sea de uso exclusivo para ir observando cómo se desempeñará y así poder detectar a temprana hora, los posibles inconvenientes que puedan surgir en la transición, para que puedan ser corregidos y estar listos para cuando se tenga que migrar toda la red.
3. En ambientes donde se tengan los dos protocolos activos, tanto IPv4 como IPv6, una manera conveniente de tener una notación para las direcciones IPv4, es colocar la dirección IPv4 en los campos más bajos de la dirección IPv6.
4. Debido a que IPsec es opcional en IPv4, es un buen momento para conocer mucho de todas las características de éste y de poder observar cómo se desempeña, para que cuando IPv6 se haya implementado se tenga un buen dominio y experiencia de éste.



## BIBLIOGRAFÍA

1. Blanchet, Marc. **Migrating to IPv6: a practical guide to implementing IPv6 in mobile and fixed networks**. Inglaterra: John Wiley & Sons Ltd., 2006. 413 pp.
2. Beijnum, Van Iljitsch. **Running IPv6**. Estados Unidos: Apress, 2006. 266 pp.
3. Hagen, Silvia. **IPv6 Essentials**. 2a ed. s.l.: O'Reilly, 2006. 230 pp.
4. Loshin, Pete. **IPv6 clearly explained**. Estados Unidos: Morgan Kaufmann Publishers, Inc., 1999. 297 pp.
5. Miller, Mark A. **Implementing IPv6**. 2a ed. Estados Unidos: M&T Books, 2000. 406 pp.
6. Stallings, William. **Comunicaciones y Redes de Computadores**. 6a ed. España: Pearson Educación, 2000. 747 pp.
7. Tanenbaum, Andrew S. **Redes de Computadoras**. 4a ed. México: Pearson Educación, 2003. 891 pp.
8. Navarro, Anna. **Diccionario de términos de comunicaciones y redes**. España: Cisco Press, 2003. 600 pp.

## REFERENCIAS ELECTRÓNICAS

9. [www.cisco.com](http://www.cisco.com) **Cisco IOS IPv6 Configuration Guide**, Release 12.4, Estados Unidos: Cisco Systems, Inc., 2008. 648 pp.
10. [www.potaroo.net/tools/ipv4](http://www.potaroo.net/tools/ipv4) 2009.
11. [www.iana.org](http://www.iana.org) 2009.
12. [www.lacnic.net/sp](http://www.lacnic.net/sp) 2009.

13. [www.rfc-editor.org](http://www.rfc-editor.org)

RFC 791. **Internet Protocol**. Estados Unidos. 1981.

RFC 792. **Internet Control Message Protocol**. 1981.

RFC 1112. **Host extensions for IP multicasting**. 1989.

RFC 1918. **Address Allocation for Private Internets**. 1996.

RFC 2401. **Security Architecture for the Internet Protocol**. 1998.

RFC 3330. **Special-Use IPv4 Addresses**. 2002.

RFC 2460. **Internet Protocol, Version 6 (IPv6) Specification**. 1998.

RFC 2402. **IP Authentication Header**. 1998.

RFC 1981. **Path MTU Discovery for IP version 6**. 1996.

RFC 4291. **IP Version 6 Addressing Architecture**. 2006.

RFC 2373. **IP Version 6 Addressing Architecture**. 1998.

RFC 3306. **Unicast-Prefix-based IPv6 Multicast Addresses**. 2002.

RFC 3956. **Embedding the Rendezvous Point (RP) Address in an IPv6 Multicast Address**. 2004.

RFC 2545. **Use of BGP-4 Multiprotocol Extensions for IPv6 Inter-Domain Routing**. 1999.

RFC 4301. **Security Architecture for the Internet Protocol**. 2005.

RFC 4303. **IP Encapsulating Security Payload (ESP)**. 2005.

RFC 3056. **Connection of IPv6 Domains via IPv4 Clouds**. 2001.

RFC 4380. **Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)** 2006.