ESCUELA POLITECNICA DEL EJÉRCITO

SEDE LATACUNGA

FACULTAD DE INGENIERIA DE SISTEMAS E

INFORMATICA

METODOLOGIA DE MIGRACION DE REDES IPV4 A IPV6
Caso Práctico: ESPE LATACUNGA

PROYECTO PREVIO A LA OBTENCION DEL TITULO DE INGENIERO DE SISTEMAS E INFORMATICA

WENDY FRANCISCA VASQUEZ ARMENDARIZ

LATACUNGA, ABRIL DE 2005

CERTIFICACION

SE CERTIFICA QUE EL PRESENTE TRABAJO FUE DESARROLLADO POR WENDY FRANCISCA VÁSQUEZ ARMENDÁRIZ, BAJO NUESTRA SUPERVISIÓN.

_____

ING. RAÚL ROSERO
DIRECTOR DE PROYECTO

_____

ING. RAÚL CAJAS
CODIRECTOR DE PROYECTO

AGRADECIMIENTO

MI MÁS SINCERA GRATITUD A DIOS, POR PERMITIRME ALCANZAR UN LOGRO MÁS EN MI VIDA Y PODER COMPARTIRLO CON MIS SERES QUERIDOS; A MIS PADRES, QUE CON AMOR Y ENTREGA TOTAL ME GUIARON, ORIENTARON Y APOYARON INCONDICIONALMENTE EN MI VIDA PERSONAL Y ACADÉMICA, Y A MIS HERMANOS QUE ESTUVIERON PRESENTES EN TODO MOMENTO.

A LA ESPE-L Y A MIS PROFESORES YA QUE ME BRINDARON SUS CONOCIMIENTOS ME FORMARON PROFESIONALMENTE Y ME ENSEÑARON EL VALOR DE LA HUMANIDAD; A MIS COMPAÑEROS QUE SIEMPRE COMPARTIERON INOLVIDABLES MOMENTOS LOS CUALES GUARDARE POR SIEMPRE EN MI CORAZÓN.

WENDY.

PRESENTACION

EL SIGUIENTE PROYECTO ESTA ORIENTADO HACIA LA NUEVA TECNOLOGÍA COMO LO ES EL PROTOCOLO IPV6, UN TEMA MUY INDISPENSABLE EN NUESTRA VIDA PROFESIONAL, Y DE GRAN AYUDA A ESTUDIANTES SIRVIENDO COMO FUENTE DE CONSULTA YA QUE BRINDA LOS CONOCIMIENTOS NECESARIOS PARA SU APLICACIÓN.

ASI COMO TAMBIEN SU CONFIGURACIÓN VENTAJAS Y ESTRUCTURA; ADEMAS UNA METODOLOGIA QUE AYUDARA A MIGRAR SIMPLIFICANDO ESTE PROCESO.

CONTENIDO

ANEXO 2.1

ENCUESTA

El siguiente cuestionario permitirá saber acerca de los conocimientos básicos que usted posee de los protocolos ipv4 e ipv6 y cuales son las expectativas que usted tiene ante lo la tecnología que nos brinda la espe-l a los docentes y estudiantes.

Estudiante ( ) Administrativo ( ) Profesor ( )

1.- ¿ conoce usted que tipo de dirección de red (clase a,b, o c) y cual es el tamaño de la dirección que se utiliza en la espe-l ?

si ( ) no ( )

2.- ¿ conoce los protocolos de enrutamiento que utiliza el protocolo ipv4 ?

Si ( ) no ( )

3.- ¿ a escuchado de las desventajas que presenta el protocolo ipv4 ?

Si ( ) no ( )

4.- ¿ a escuchado sobre en nuevo protocolo ipv6 y las ventajas que nos presentaría este al utilizarlo?

Si ( ) no ( )

5.- ¿ sabía que el tamaño de dirección del protocolo ipv6 es de 8 bits ?

Si ( ) no ( )

6.- ¿ sabía que el nuevo protocolo ipv6 tiene diferente forma de enrutamiento de los paquetes que el protocolo ipv4 ?

Si ( ) no ( )

7.-¿ conoce o a escuchado sobre alguna técnica de migración de redes ipv4 a redes ipv6?

Si ( ) no ( )

8.- ¿ de las técnicas de migración, sabe usted cual es la más utilizada o recomendada ?

Si ( ) no ( )

9.- ¿ desearía que la espe -l empleará este el nuevo protocolo ?

Si ( ) no ( )
porqué……..……..……

ANEXO 2.2

ENTREVISTAS

NOMBRE:

1.- A TENIDO ALGÚN PROBLEMA CON LOS SERVICIOS O AL UTILIZAR EL PROTOCOLO IPV4

……
……
……
……

2.- SABE USTED EL TAMAÑO Y VENTAJAS QUE NOS BRINDA EL PROTOCOLO IPV6

……
……
……
……
……

3.- CONOCE ALGUNA TÉCNICA DE MIGRACIÓN O SABE CUAL DE ESTAS SE A EMPLEADO EN ALGUNA INSTITUCIÓN

……
……
……
……

4.- CREE QUE SE DEBERÍA IMPLANTAR IPV6 Y QUE BENEFICIOS CREE QUE TRAERÁ LA IMPLANTACIÓN ESTE PROTOCOLO EN LA RED DE LA ESPE-L

……
……
……
……
……

5.- CONSIDERA NECESARIO LA MIGRACIÓN AL NUEVO PROTOCOLO IPV6 Y POR QUE

……
……
……
……
……

6.- PIENSA QUE TODOS LOS SERVICIOS QUE NOS BRINDA EL NUEVO PROTOCOLO AYUDARÁ A LAS REDES, ESTUDIANTES O SERVICIOS QUE OFRECE LA ESPE-L

……
……
……
……
……

ANEXO 3.1

COMANDOS BASICOS DE IPV6 BAJO LINUX

Mostrar direcciones ipv6

Se puede hacer mediante el uso de **ip** o **ifconfig**:

#> /sbin/ip -6 addr show dev <interface>

#> /sbin/ifconfig <interface>

Añadir una dirección ipv6

Se puede hacer mediante el uso de **ip** o **ifconfig**:

#> /sbin/ip -6 addr add <ipv6address>/<prefixlength> dev <interface>

#> /sbin/ifconfig <interface> inet6 add <ipv6address>/<prefixlength>

Eliminar una dirección ipv6

Se puede hacer mediante el uso de **ip** o **ifconfig**:

#> /sbin/ip -6 addr del <ipv6address>/<prefixlength> dev <interface>

#> /sbin/ifconfig <interface> inet6 del <ipv6address>/<prefixlength>

Mostrar rutas ipv6

Se puede hacer mediante el uso de **ip** o **route**:

#> /sbin/ip -6 route show [dev <device>]

#> /sbin/route -a inet6

Añadir una ruta ipv6 a través de un gateway

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route add <ipv6network>/<prefixlength> via <ipv6address>
[dev <device>]

#> /sbin/route -a inet6 add <ipv6network>/<prefixlength> gw <ipv6address> [dev <device>]

Eliminar una ruta ipv6 a través de un gateway

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route del <ipv6network>/<prefixlength> via <ipv6address> [dev <device>]

#> /sbin/route -a inet6 del <ipv6network>/<prefixlength> gw <ipv6address> [dev <device>]

Añadir una ruta ipv6 a través de una interfaz

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route add <ipv6network>/<prefixlength> dev <device> metric 1

#> /sbin/route -a inet6 add <network>/<prefixlength> dev <device>

Eliminar una ruta ipv6 a través de una interfaz

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route del <ipv6network>/<prefixlength> dev <device> metric 1

#> /sbin/route -a inet6 del <network>/<prefixlength> dev <device>

Ping6

Normalmente incluido en el paquete iputils. Uso:

#> ping6 <hostwithipv6address>

#> ping6 <ipv6address>

#> ping6 [-i <device>] <link-local-ipv6address>

Traceroute6

Normalmente incluido en el paquete iputils. Uso:

#>traceroute6

Tracepath6

Normalmente incluido en el paquete iputils. Uso:

#>tracepath6

ANEXO 3.2

COMANDOS BASICOS DE IPV6 BAJO WINDOWS

- **Ipv6 install**

  Instala el protocolo ipv6 como protocolo de red para conexiones lan.

  Ipv6 uninstall

  Quita el protocolo ipv6 como protocolo de red para conexiones lan.

- **Ipv6** [**-v**] **if** [*índicedeinterfaz*]

  Muestra información acerca de las interfaces.

- **Ipv6 ifcr v6v4** *origenv4 destinov4* [**nd**] [**pmld**]

  Crea una interfaz configurada de túnel ipv6 sobre ipv4 con las direcciones ipv4 de origen y destino especificadas.

- **Ipv6 ifcr 6over4** *origenv4*

  Crea una interfaz para 6over4 con la dirección ipv4 de origen especificada. Para obtener más información acerca de 6over4, consulte el documento rfc 2529.

- **Ipv6 ifc** *índicedeinterfaz* {[**forwards**] | [**-forwards**]} {[**advertises**] | [**-advertises**]} [**mtu** *númerodebytes*] [**site** *identificadordesitio*]

  Controla los atributos de la interfaz.

- **Ipv6 ifd** *índicedeinterfaz*

Elimina una interfaz. Las pseudointerfaces de bucle de retroceso y de túnel automático no se pueden eliminar.

- **Ipv6 adu** *índicedeinterfaz***/***dirección* [**life** *duraciónválida*[**/***duraciónpreferida*]] [**anycast**] [**unicast**]

  Agrega o quita la asignación de una dirección de unidifusión o de difusión por proximidad en una interfaz, con el valor predeterminado de unidifusión a menos que se especifique difusión por proximidad.

- **Ipv6 nc** [*índicedeinterfaz* [*dirección*]]

  Muestra el contenido de la caché de vecinos.

- **Ipv6 ncf** [*índicedeinterfaz* [*dirección*]]

  Quita las entradas especificadas de la caché de vecinos.

- **Ipv6 rc** [*índicedeinterfaz* [*dirección*]]

  Muestra el contenido de la caché de enrutamiento.

- **Ipv6** [**-v**] **rt**

  Muestra el contenido actual de la tabla de enrutamiento.

- **Ipv6 rtu** *prefijo índicedeinterfaz*[**/***dirección*]]

  Agrega o quita una ruta en la tabla de enrutamiento.

- **Ipv6 spt**

  Muestra el contenido de la tabla de prefijos del sitio.

- **Ipv6 spu** *prefijo índicedeinterfaz* [**life** */*]

Agrega, quita o actualiza un prefijo en la tabla de prefijos del sitio.

- **Ipv6 gp**

  Muestra los valores de los parámetros globales del protocolo ipv6.

- **Ipv6** [**-p**] **gpu defaultcurhoplimit** *saltos*

  Establece el valor del campo límite de saltos del encabezado ipv6 en los paquetes enviados por el nodo.

- **Ipv6** [**-p**] **gpu useanonymousaddresses** [**yes**|**no**|**always**|*contador*]

  Determina si se utilizan o no direcciones anónimas. El valor predeterminado es **yes**. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu maxanondadattempts** *número*

  Establece el número de veces que se comprueba si una dirección anónima es única. El número predeterminado de intentos es 5. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu maxanonlifetime** *válida*[/*preferida*]

  Establece la duración válida y la duración preferida de las direcciones anónimas. La duración válida predeterminada es de 7 días. La duración preferida predeterminada es de 1 día. La opción **-p** guarda las opciones en el registro.

- **Ipv6** [**-p**] **gpu anonregeneratetime** *tiempo*

  Establece el período de tiempo (en segundos) en el que se debe generar una nueva dirección anónima. El valor predeterminado es de 5 segundos. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu maxanonrandomtime** *tiempo*

  Establece la cantidad de tiempo en minutos del tiempo aleatorio anónimo máximo. El tiempo aleatorio anónimo es el periodo de tiempo que transcurre hasta que caduca el periodo de tiempo válido en el que una dirección anónima puede generar una nueva dirección anónima. El protocolo ipv6 de windows xp elige aleatoriamente un tiempo aleatorio anónimo entre los valores de anonrandomtime y maxanonrandomtime. El escalonado aleatorio de la regeneración de direcciones anónimas se realiza para evitar repercusiones negativas en el tráfico de red cuando muchas direcciones anónimas dejan de ser válidas simultáneamente. El valor predeterminado es de 10 minutos. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu anonrandomtime** *tiempo*

  Establece el tiempo aleatorio anónimo mínimo en segundos. El valor predeterminado es de 0 segundos. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu neighborcachelimit** *número*

  Establece el número máximo de entradas de la caché de vecinos para cada interfaz. El valor predeterminado es de 8 entradas. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu routecachelimit** *número*

  Establece el número máximo de entradas de la caché de enrutamiento para cada interfaz. El valor predeterminado es de 32 entradas. La opción **-p** guarda el valor en el registro.

- **Ipv6 ppt**

Muestra la tabla de directivas de prefijos. La tabla de directivas de prefijos se utiliza para especificar las directivas de selección de direcciones de origen y destino.

- **IPV6 PPU** *PREFIJO* **PRECEDENCE** *VALORDEPRIORIDAD* **SRCLABEL** *valordeetiquetadeorigen* [**dstlabel** *valordeetiquetadedestino*]

  Actualiza la tabla de directivas de prefijos con una directiva que especifica la prioridad, un valor de etiqueta de origen (*valordeetiquetadeorigen*) y un valor de etiqueta de destino (*valordeetiquetadedestino*). Las entradas de la tabla de directivas de prefijos pueden modificar el comportamiento de la selección de direcciones de origen y destino. Para obtener más información, consulte el borrador de internet titulado "default address selection for ipv6" (selección de direcciones predeterminadas en ipv6).

- **IPV6 RENEW** [*ÍNDICEDEINTERFAZ*]

  Renueva la configuración de ipv6 en todas las interfaces. Si se especifica un número de índice de interfaz, sólo se renovará la configuración de esa interfaz. Para un host, las direcciones configuradas automáticamente se actualizan enviando mensajes de solicitud de enrutador en las interfaces correspondientes. Las direcciones se vuelven a configurar en función de los mensajes de anuncio de enrutador recibidos.

CAPITULO I

INTRODUCCION A LOS PROTOCOLOS IPV4 E IPV6

1.1.- BREVE HISTORIA DE TCP/IP

TCP/IP fue diseñado a finales de los 60's como el fundamento de la red ARPANET que conectaba las computadoras de oficinas gubernamentales y universitarias.

La necesidad surge a partir de que el Departamento de Defensa de los Estados Unidos de América (DoD) al ver que no era suficiente la comunicación entre sus computadoras y que necesitaba tener conexión con contratistas y organizaciones implicadas en investigaciones.

De ahí en adelante se inició la investigación para desarrollar productos de red, y tecnología de comunicación que hoy se denomina *conmutación de paquetes* y por ende aparece el protocolo TCP/IP a inicios de 1969. Entre los objetivos principales se encontraban los siguientes:

- **Protocolos Comunes**: Quería un protocolo común que pudiera comunicarse todas las redes y simplificar los procesos.
- **Interoperabilidad**: Los equipos de distintos fabricantes pudieran funcionar conjuntamente, el desarrollo sería más eficiente y se fomentaría la competitividad entre los proveedores.
- **Comunicaciones sólidas:** Los protocolos debían proporcionar conexiones fiables y de alto rendimiento utilizando las tecnologías de redes de área extensa relativamente primitivas que estaba disponible en aquel momento.
- **Facilidad de reconfiguración:** Poder reconfigurar la red, poder añadir o eliminar computadoras sin interrumpir las comunicaciones.

ARPANET a partir de entonces inició la investigación sobre redes utilizando la tecnología que hoy se denomina "*intercambio de paquetes"* evolucionando para lo que ahora se conoce como INTERNET y con ello también evolucionó el protocolo TCP/IP que hoy en día está ampliamente difundida.

1.2.- INTRODUCCIÓN A REDES

A principios de los años 70 surgieron las primeras redes de transmisión de datos destinadas exclusivamente a este propósito, cumpliendo con las necesidades de funcionalidad, flexibilidad y economía que en ese momento se requería. Se comenzaron a considerar las ventajas de permitir la comunicación entre computadoras y entre grupos de terminales, y de ser posible compartir recursos en mayor o menor grado.

1.3.- CONCEPTOS DE RED

Una red de computador es una serie de PCs y otros dispositivos conectados por cables entre sí. Esta conexión permite comunicarse entre ellos y compartir información y recursos. Las redes varían en tamaño; pueden reducirse a una oficina o extenderse globalmente.

Una red debe ser:

- **Confiable**: Estar disponible cuando se le requiera, poseer velocidad de respuesta adecuada.
- **Confidencial:** Proteger los datos sobre los usuarios de ladrones de información.
- **Integra:** En su manejo de información.

1.3.1.- Red cliente/servidor

Es una estructura de red de área local (LAN), en la que los recursos de red están centralizados y controlados desde uno o más servidores. Las estaciones de trabajo

individuales o *clientes* (como son los PCs) deben solicitar los servicios a través del/los servidor/es.

1.3.2.- Red de igual a igual

Una red de igual a igual o red punto a punto es aquella en la que las estaciones de trabajo (como los PCs) pueden compartir información y los recursos de todos ellos, sin tener que depender de un servidor central.

1.3.3.- Red Inalámbrica

Red de área local inalámbrica (Wireless Local Area Network) es un entorno de red en el cual usuarios, dispositivos periféricos, Internet o dispositivos de encaminamiento están conectados por medio de una conexión inalámbrica.

1.3.4.- Normas para Redes (IEEE 802.X)

Es un conjunto de normas que definen las características físicas de las redes, dictadas por el IEEE (Institute of Electrical and Electronic Engineers). En estas normas también se define el control de acceso al medio (MAC). Las normas son las siguientes:

- √ **802.1 -** Estándar definido relativo a los algoritmos para enrutamiento de cuadros o frames (la forma en que se encuentra la dirección destino).
- √ **802.2 -** Define los métodos para controlar las tareas de interacción entre la tarjeta de red y el procesador llamado LLC.
- √ **802.3 -** Define las formas de protocolos Ethernet CSMA/CD (**C**arrier-**s**ense **M**ultiple **A**ccess with **C**ollision **D**etection) en sus diferentes medios físicos (cables).
- √ **802.4 -** Define cuadros Token Bus tipo ARCNET.
- √ **802.5 -** Define hardware para Token Ring.

- √ **802.6 -** Especificación para redes tipo MAN.
- √ **802.7 -** Especificaciones de redes con mayores anchos de banda con la posibilidad de transmitir datos, sonido e imágenes.
- √ **802.8 -** Especificación para redes de fibra óptica time Token Passing/FDDI (Fiber data Distribution Interface).
- √ **802.9 -** Especificaciones de redes digitales que incluyen video.
- √ **802.11** - Estándar para redes inalámbricas con línea visual.
- √ **802.11a** - Estándar superior al 802.11b, pues permite velocidades teóricas máximas de hasta 54 Mbps, apoyándose en la banda de los 5GHz. A su vez, elimina el problema de las interferencias múltiples que existen en la banda de los 2,4 GHz.
- √ **802.11b** - Extensión de 802.11 para proporcionar 11 Mbps. También conocido comúnmente como Wi-Fi (Wireless Fidelity): Es el estándar más utilizado en las comunidades inalámbricas.
- √ **802.11e** - Estándar encargado de diferenciar entre video-voz-datos. Su único inconvenientes el encarecimiento de los equipos.
- √ **802.11g -** Utiliza la banda de 2,4 GHz, pero permite transmitir sobre ella a velocidades teóricas de 54 Mbps.
- √ **802.11i -** Conjunto de referencias en el que se apoyará el resto de los estándares, en especial el futuro 802.11a. El 802.11i supone la solución al problema de autenticación al nivel de la capa de acceso al medio, pues sin ésta, es posible crear ataques de denegación de servicio (DoS).
- √ **802.12 -** Comité para formar el estándar do 100 base VG quo sustituye CSMA/CD por asignación de prioridades.
- √ **802.14 -** Comité para formar el estándar de 100 base VG sin sustituir CSMA/CD.

1.4.- TOPOLOGIAS

La topología define la estructura de una red. La definición de topología puede dividirse en dos partes. La topología física que es la disposición real de los cables

(los medios) y la topología lógica, que define la forma en que los host (equipos) acceden a los medios.

Las topologías físicas mas utilizadas son:

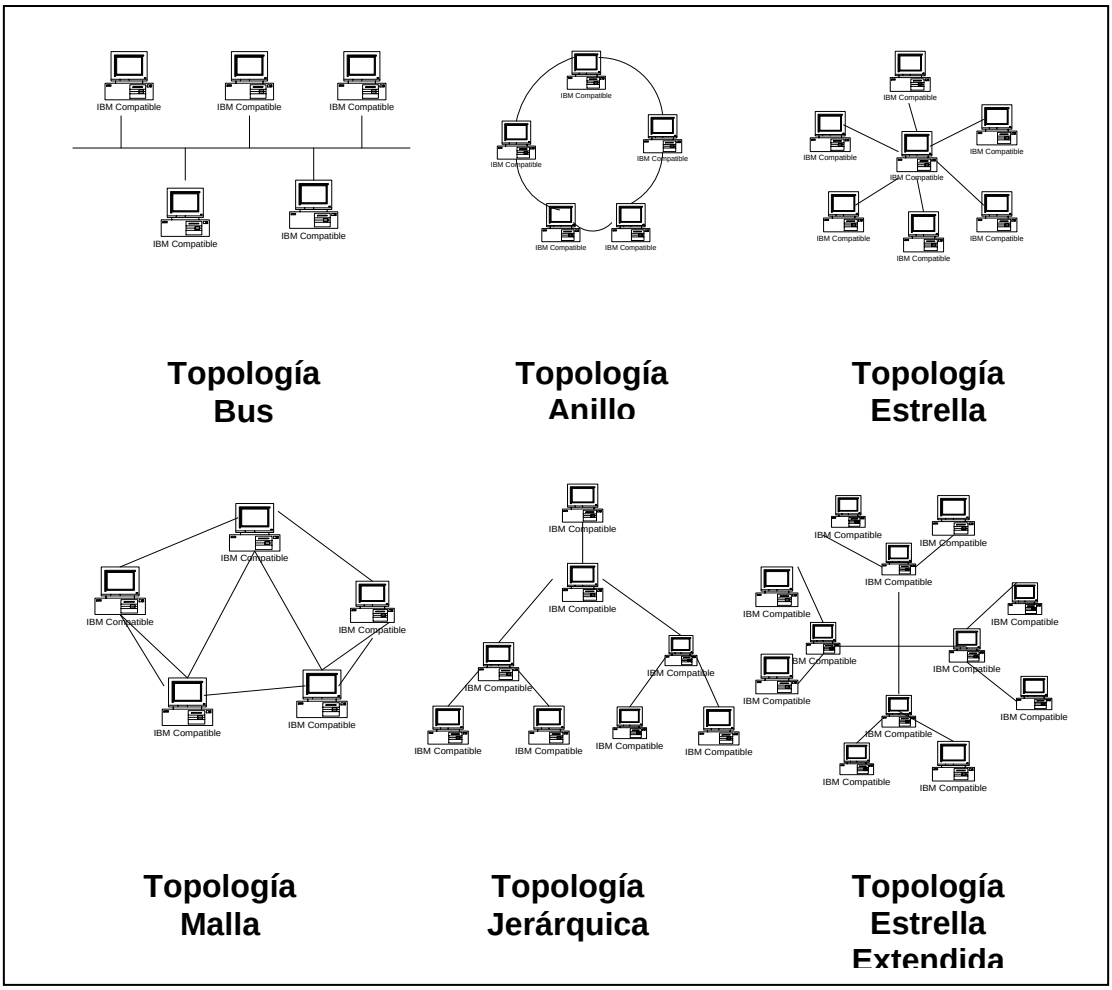


Grafico 1.1 Tipos de Topologías

1.4.1.- TOPOLOGÍA DE TIPO BUS

A menudo, recibe el nombre de «bus lineal», porque los equipos se conectan en línea recta. Éste es el método más simple y común utilizado en las redes de equipos. Consta de un único cable llamado segmento central (trunk; también

llamado backbone o segmento) que conecta todos los equipos de la red en una única línea. Como es bastante simple la configuración, se puede implementar de manera barata. El problema inherente de este esquema es que si el cable se daña en cualquier punto, ninguna estación podrá transmitir. Aunque Ethernet puede tener varias configuraciones de cables.

1.4.2.- TOPOLOGÍA DE TIPO ESTRELLA

En la topología en estrella, los segmentos de cable de cada equipo están conectados a un componente centralizado llamado hub. Las señales son transmitidas desde el equipo emisor a través del hub a todos los equipos de la red.

La red en estrella ofrece la ventaja de centralizar los recursos y la gestión. Sin embargo, como cada equipo está conectado a un punto central, esta topología requiere una gran cantidad de cables en una gran instalación de red. Además, si el punto central falla, cae toda la red.

1.4.3.- TOPOLOGÍA TIPO ANILLO

La topología en anillo conecta equipos en un único círculo de cable. A diferencia de la topología en bus, no existen finales con terminadores. La señal viaja a través del bucle en una dirección, y pasa a través de cada equipo que puede actuar como repetidor para amplificar la señal y enviarla al siguiente equipo. El fallo de un equipo puede tener impacto sobre toda la red.

Conocida también como token ring, es parecida a la topología estrella pero con un dispositivo llamado MAU (Multi Access Unit). Existe una topología de anillo conocida como FDDI (Fiber data Distribution Interface), puede contar con dos MAU (dual Homed) y opera sobre fibra óptica.

1.4.4.- TOPOLOGÍA TIPO MALLA

Ofrece redundancia y fiabilidad. En una topología en malla, cada equipo está conectado a todos los demás equipos mediante cables separados. Esta configuración ofrece caminos redundantes por toda la red, de modo que si falla un cable, otro se hará cargo del tráfico. Aunque la facilidad de solución de problemas y el aumento de la fiabilidad son ventajas muy interesantes, estas redes resultan caras de instalar, ya que utilizan mucho cableado. En muchas ocasiones, se utiliza junto con otras topologías para formar una topología híbrida.

1.4.5- TOPOLOGÍA TIPO GERARQUICA

Es una de las más utilizadas en redes WAN, consiste en la distribución jerárquica de las unidades en un bus donde la información tiene que llegar siempre a la cabecera de jerarquía.

1.4.6- TOPOLOGÍA TIPO ESTRELLA EXTENDIDA

Esta red incluye redes tipo estrella entre sí por medio de un dispositivo integrado que generalmente es un conmutador o switch.

1.5.- REDES LAN (Local Area Network)

Son redes pequeñas entendiendo como pequeñas las redes de una oficina de un edificio o Campus de una Universidad, debido a sus limitadas dimensiones, son muy rápidas y cada estación se puede comunicar con el resto. Suelen emplear conectores y cableado al que están conectadas todas las máquinas. Sin embargo no son simples en diseño ya que pueden conectar cientos de computadoras y ser utilizadas por cientos de usuarios.

La estructura de red de una (LAN), están centralizados y controlados desde uno o más servidores. Las estaciones de trabajo individuales o *clientes* (como son los PCs) deben solicitar los servicios a través del/los servidor/es.

Hay varias tecnologías LAN, siendo Ethernet[1] y Fast Ethernet[2] las más comunes. Una red puede estar basada en una o más de estas tecnologías. Las redes Ethernet y Fast Ethernet utilizan un protocolo llamado CSMA/CD (**C**arrier-**s**ense **M**ultiple **A**ccess with **C**ollision **D**etection). (Acceso múltiple del sentido de portadora con detección de colisión). Este protocolo no permite que más de un dispositivo comunique al mismo tiempo.

1.6.- REDES WAN (Wide Area Network)

Una Red de área extensa (WAN) es un grupo de dispositivos, o varias LAN, conectados en una área geográficamente mayor, a menudo por medio de líneas telefónicas u otro formato de cableado como puede ser una línea dedicada de alta velocidad, fibra o enlace vía satélite. Uno de los mayores ejemplos de WAN es la propia Internet. Estas redes tienen menor velocidad aunque son capaces de transportar mayor cantidad de datos.

Una WAN le permite compartir recursos e información a lo largo de un área geográficamente mayor, examinar la Web o transferir archivos y mensajes por correo electrónico.

INTERNET: Es una red global compuesta por redes gubernamentales, académicas, comerciales, Militares y corporativas que abarcan todo el mundo. Los

[1] Tecnología utilizada extensamente en las LANs. Las redes de Ethernet utilizan el protocolo CSMA/CD y funcionan en varios cables a una velocidad de 10Mbps; son utilizados por protocolos TCP/IP. Ethernet es similar a una serie de normas producidas por IEEE, conocidas como IEEE 802.3.

[2] Las redes de Fast Ethernet operan a una velocidad de 100Mbps, y se basan en el método de acceso a red 10 BASE-T Ethernet CSMA/CD, extensión de la norma IEEE 802.3.

usuarios que tienen acceso a Internet pueden leer y descargar datos, virtualmente acerca de cualquier tema, desde casi cualquier parte del mundo.

1.7.- COMPONENTES

1.7.1.- SERVIDORES

Es un computador o dispositivo especializado en una red que comparten usuarios múltiples. Un servidor facilita a los usuarios el acceso a servicios de red compartidos, tales como ficheros del computador e impresoras, etc.

1.7.2.- CLIENTES

Son los computadores conectados al servidor. Los clientes no han de ser tan potentes como el servidor, simplemente necesita una tarjeta de red, el cableado pertinente y el software necesario para comunicarse con el servidor. Un cliente puede carecer de disquetera y de disco duro y trabajar directamente sobre el servidor. Prácticamente cualquier PC puede actuar como estación de trabajo.

1.7.3.- TARJETA DE RED (NICs)

Las tarjetas de interfaz de red (NIC) son utilizadas en operaciones en red; Ya que esta depende de aspectos importantes como: La velocidad de su conexión, o servidor de impresora; entre las velocidades tenemos Ethernet (10Mbps) o Fast Ethernet (100Mbps), El tipo de conexión que necesita es (RJ-45) para par trenzado, fibra óptica o inalámbrica.

1.7.4.- VELOCIDAD DE CONEXIÓN

Dentro de la velocidad de conexión se recomienda utilizar tarjetas de red de Ethernet con un concentrador o conmutador Ethernet, y tarjeta de red Fast Ethernet con un concentrador o conmutador Fast Ethernet.

También se pueden emplear dispositivo dual speed que admite ambos valores, 10 y 100Mbps, Un puerto en un dispositivo dual speed ajusta su velocidad automáticamente para que coincida con la velocidad más alta admitida por ambos extremos de la conexión.

Nota: Los dispositivos dual speed se conocen también como dispositivos autonegociadores, autosensings o 10/100.

1.7.5.- CONMUTADORES (SWITCH)

Un switch solamente envía información cuando es necesario (a diferencia del concentrador, que envía información a todos sus puertos). Una vez que aprende qué dispositivos pueden alcanzarse a través de cada puerto, el conmutador (switch) solamente pasará paquetes a los puertos adecuados. De este modo, un conmutador puede reducir la cantidad de tráfico en gran medida, y mejorar el rendimiento de la red. Un conmutador (Switch), se utiliza generalmente para conectar concentradores entre sí, o para facilitar conexiones dedicadas a estaciones de alto rendimiento.

1.7.6.- CONCENTRADORES (HUB)

Uno de los componentes de las redes que se ha convertido en un dispositivo estándar en las mismas es el hub.

Hubs activos: La mayoría de los hubs son activos; es decir, regeneran y retransmiten las señales del mismo modo que un repetidor. Generalmente los hubs tienen de ocho a doce puertos para conexión de equipos de la red, a menudo se les llama repetidores multipuerto. Los hubs activos requieren corriente eléctrica para su funcionamiento.

Hubs pasivos: Algunos tipos de hubs son pasivos; como ejemplos están los paneles de conexión o los bloques de conexión (punch-down blocks). Actúan como

puntos de conexión y no amplifican o regeneran la señal; la señal pasa a través del hub. Los hubs pasivos no necesitan corriente eléctrica para funcionar.

Hubs híbridos: Los hubs híbridos son hubs avanzados que permiten conectar distintos tipos de cables.

1.7.7.- MÓDEMS

Modulador-Demodulador. Es un dispositivo que adapta la señal digital de un computador en frecuencias de sonido (análógicas) para transmitir a través de una línea de teléfono, y las adapta de nuevo a digitales. Las velocidades de transmisión de los módems se sitúan generalmente entre los 2.400bps (2.4Kbps) a los 56.000bps (56Kbps).

1.7.8- ROUTERS

Los routers trabajan en el nivel de red del modelo de referencia OSI. Esto significa que pueden conmutar y encaminar paquetes a través de múltiples redes. Realizan esto intercambiando información específica de protocolos entre las diferentes redes. Los routers leen en el paquete la información de direccionamiento de la redes complejas teniendo acceso a información adicional, puesto que trabajan a un nivel superior del modelo OSI.

1.7.9- SISTEMAS OPERATIVOS DE RED

El Computador tiene un sistema operativo de red que le permite ofrecer servicios a través de la red, a otros usuarios.

Existen diferentes tipos de sistemas operativos de red. Por ejemplo, Microsoft ha creado una serie de sistemas operativos entre los que se cuentan: *Windows 98, Windows xp*, *Windows NT*, *Windows 2000 server, Windows 2003 server* etc. Estos

sistemas operativos se comunican con otros dispositivos en su red utilizando un conjunto de normas. Estas normas se conocen como *Protocolos*.

1.8.- VISION GLOBAL DE LA INTRANET

Las Intranets son redes privadas internas, utilizadas por compañías e instituciones académicas alrededor del mundo. El público del exterior no puede acceder a estas Intranets, que sirven como bases de datos de información en el mismo formato que utiliza la World Wide Web.

Las Intranets brindan a los usuarios la capacidad de compartir dinámicamente recursos internos de la misma forma que los usuarios de Internet lo hacen. Para usar una Intranet, las computadoras cliente normalmente necesitan de:

- Protocolo (TCP/IP) instalado
- Un navegador de Web
- Un servidor de Web.

1.9.- LA INTRANET EN LA ESPE-L

La Escuela Politécnica del Ejercito sede Latacunga emplea la tecnología IPv4 dado que la nueva generación Ipv6 no ha cubierto completamente a Latinoamérica y mucho menos a Ecuador. La estructura física de la intranet de la institución consta de tres servidores:

- Primer Servidor empleado para aplicaciones.
- Segundo Servidor empleado para Usuarios.
- Tercer Servidor empleado para uso de Internet, Firework y correo.

Todos estos servidores se encuentran conectados a los departamentos y oficinas por medio de cable UTP categoría 5 E y fibra Óptica;

1.10.- TCP/IP EN LAS INTRANETS

Una intranet no es más que una red local funcionando como lo hace Internet, es decir usando el conjunto de protocolos TCP/IP en sus respectivos niveles. Este concepto engloba a todo un conjunto de redes locales con distintas topologías y cableados, pero que en sus niveles de transporte y de red funcionan con los mismos protocolos.

Este hecho, facilita enormemente la conexión con otros tipos de redes a través de Internet, puesto que utiliza sus mismos protocolos. Además todas las herramientas y utilidades que existen para Internet, se pueden utilizar en una intranet (creación de páginas Web, correo electrónico).

No es lo mismo interconectar dos Intranets con la misma arquitectura que dos Intranets de arquitecturas diferentes y con diferentes protocolos

1.11.- FUNCION DE LOS COMPONENTES EN LAS INTRANETS

1.11.1.- CONCENTRADORES (HUB) Y CONMUTADORES (SWITCH)

Los Hub y switch se utilizan para conectar sus PCs, impresoras y otros dispositivos.

Los hub se diferencian de los switch en el modo en el que administran el tráfico[3] de la red.

[3] Movimiento de paquetes de datos en una red.

Los hub se pueden utilizar para ampliar una red. No obstante, de esta acción puede resultar un exceso de tráfico innecesario porque se envía la misma información a todos los dispositivos de una red.

Los switch están indicados para redes pequeñas, aunque es posible que las redes con alta carga de tráfico necesiten equipos de red adicionales, como puede ser un conmutador, que reduciría el tráfico innecesario.

Los switch utilizan la información de la dirección de cada paquete para controlar el flujo del tráfico de la red. Por medio de la monitorización de los paquetes que recibe, un switch distingue qué dispositivos están conectados a sus puertos[4], y envía los paquetes a los puertos adecuados solamente.

Un switch reduce la cantidad de tráfico innecesario porque la información recibida en un puerto se envía solamente al dispositivo que tiene la dirección de destino correcta, a diferencia de un concentrador o hub , que la envía a todos los puertos.

Los conmutadores y los concentradores se utilizan a menudo en la misma red. los concentradores expanden la red añadiendo más puertos, y los conmutadores dividen la red en secciones más pequeñas y menos congestionadas.

En una red pequeña, los concentradores pueden ocuparse fácilmente de todo el tráfico generado.

Cuando la red llega a tener alrededor de 25 usuarios, es posible que tenga que reducir el tráfico innecesario.

Cuando se añaden concentradores a la red, hay una serie de normas que deben conocerse acerca del número de concentradores que se pueden conectar a la vez. Los conmutadores se pueden utilizar para extender el número de concentradores en la red.

[4] Es un zócalo desde el que los datos pueden entrar y salir de un computador, o de un dispositivo componente de una red.

1.11.2.- MÓDEMS, ROUTERS Y FIREWALLS

La velocidad a la que un módem transmite se mide en Kbps[5]. La mayoría de los módems utilizados hoy en día transmiten a velocidades que varían entre los 28.8Kbps y los 56Kbps. Los módems también se definen según su norma ITU (Unión de Telecomunicaciones Internacional).

En una red, un firewall es un nodo configurado como una barrera para impedir que el tráfico cruce de un segmento a otro. Los firewalls también mejoran la seguridad de la red y pueden servir como barrera en las conexiones entre las redes públicas y privadas. Un firewall puede ser implementado en un router o puede ser un dispositivo de red especial para este propósito.

1.12.- ESPECIFICACIONES BÁSICAS DE IPV4

El protocolo IP (Internet Protocol) fue diseñado para interconexión de redes. IP se ocupa de la transmisión de bloques de datos, llamados datagramas de origen a destino, donde orígenes y destinos son *clientes o host* identificados por direcciones de una longitud fija.

IP también se encarga de la fragmentación y reensamblado de datagramas, si éste fuera necesario. El módulo Internet usa las direcciones contenidas en la cabecera de los datagramas para hacer llegar a estos a sus destinos. Asimismo, existen otros campos en la cabecera que permiten gestionar la fragmentación y posterior reensamblado de datagramas, para poder transmitir a través de redes que trabajen con tamaños de paquete pequeños.

---

[5] **K**ilo**b**its **p**or **s**egundo. Es la medida de la velocidad de transferencia de datos en un sistema de comunicaciones. Un kilobit equivale a 1000 bits

Un datagrama es la unidad básica de transferencia entre la Internet, y se descompone en cabecera y datos.

El IP es un protocolo que pertenece al nivel de red del modelo OSI, por lo tanto, es utilizado por los protocolos del nivel de transporte como TCP para encaminar los datos hacia su destino. Suponiendo que el protocolo TCP ha sido el encargado de manejar el datagrama antes de pasarlo al IP, la estructura del mensaje una vez tratado quedaría así:

Cabecera IP (20 byte)	**Cabecera TCP (20 byte)**	**Datos**	

Tabla 1.1: Formato del Datagrama de TCP/IP[6]

La estructura de un datagrama IPv4 es la siguiente:

Bits 4 8 16 20 32

Versión	**Cabecera**	**TOS**	**Longitud Total**	
Identificación			**Indicador**	**Desplazamiento de Fragmentación**
TTL		**Protocolo**	**Checksum**	
Dirección Fuente 32 bits				
Dirección Destino 32 bits				
Opción				

Figura 1.1: Formato de la cabecera IPv4[7]

[6] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

- **Versión**: Número de versión del protocolo IP utilizado. Tendrá que tener el valor 4. Tamaño: 4 bit.
- **Longitud de la cabecera:** (Internet Header Length, IHL) Especifica la longitud de la cabecera expresada en el número de grupos de 32 bit que contiene. Tamaño: 4 bit.
- **Tipo de servicio:** El tipo o calidad de servicio se utiliza para indicar la prioridad o importancia de los datos que se envían, lo que condicionará la forma en que éstos serán tratados durante la transmisión. Tamaño: 8 bit.
- **Longitud total:** Es la longitud en bytes del datagrama completo, incluyendo la cabecera y los datos. Como este campo utiliza 16 bit, el tamaño máximo del datagrama no podrá superar los 65.535 bytes, aunque en la práctica este valor será mucho más pequeño. Tamaño: 16 bit.
- I**dentificación:** Valor de identificación que se utiliza para facilitar el ensamblaje de los fragmentos del datagrama. Tamaño: 16 bit.
- **Flags:** Indicadores utilizados en la fragmentación. Tamaño: 3 bit.
- **Fragmentación:** Contiene un valor (offset) para poder ensamblar los datagramas que se hayan fragmentado. Está expresado en número de grupos de 8 bytes (64 bit), comenzando con el valor cero para el primer fragmento. Tamaño: 16 bit.
- **Límite de existencia:** Contiene un número que disminuye cada vez que el paquete pasa por un sistema. Si este número llega a cero, el paquete será descartado. Esto es necesario por razones de seguridad para evitar un bucle infinito, ya que aunque es bastante improbable que esto suceda en una red correctamente diseñada, no debe descuidarse esta posibilidad. Tamaño: 8 bit.
- **Protocolo:** El número utilizado en este campo sirve para indicar a qué protocolo pertenece el datagrama que se encuentra a continuación de la

---

[7] http://long.ccaba.upc.es/long/050Dissemination_Activities/carlos_ralli_transitiontutorial.pdf

cabecera IP, de manera que pueda ser tratado correctamente cuando llegue a su destino. Tamaño: 8 bit.

- **Comprobación:** El campo de comprobación (checksum) es necesario para verificar que los datos contenidos en la cabecera IP son correctos. Por razones de eficiencia este campo no puede utilizarse para comprobar los datos incluidos a continuación, sino que estos datos de usuario se comprobarán posteriormente a partir del campo de comprobación de la cabecera siguiente, y que corresponde al nivel de transporte. Este campo debe calcularse de nuevo cuando cambia alguna opción de la cabecera, como puede ser el límite de existencia. Tamaño: 16 bit.
- **Dirección de origen:** Contiene la dirección del host que envía el paquete. Tamaño: 32 bit.
- **Dirección de destino:** Esta dirección es la del host que recibirá la información. Los routers o gateways intermedios deben conocerla para dirigir correctamente el paquete. Tamaño: 32 bit.

El protocolo IP identifica a cada computador que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bit que debe ser único para cada host, y normalmente suele representarse como cuatro cifras de 8 bit separadas por puntos.

La dirección de Internet (IP Address) se utiliza para identificar tanto al computador en concreto como la red a la que pertenece, de manera que sea posible distinguir a los computadores que se encuentran conectados a una misma red. Con este propósito, y teniendo en cuenta que en Internet se encuentran conectadas redes de tamaños muy diversos, se establecieron tres clases diferentes de direcciones, las cuales se representan mediante tres rangos de valores:

Clase A: Son las que en su primer byte tienen un valor comprendido entre 1 y 126, incluyendo ambos valores. Estas direcciones utilizan únicamente este primer byte para identificar la red, quedando los otros tres bytes disponibles para cada uno de los hosts que pertenezcan a esta misma red. Esto significa que podrán existir más

de dieciséis millones de computadores en cada una de las redes de esta clase. Este tipo de direcciones es usado por redes muy extensas, pero hay que tener en cuenta que sólo puede haber 126 redes de este tamaño. ARPAnet es una de ellas, existiendo además algunas grandes redes comerciales, aunque son pocas las organizaciones que obtienen una dirección de "clase A". Lo normal para las grandes organizaciones es que utilicen una o varias redes de "clase B".

Clase B: Estas direcciones utilizan en su primer byte un valor comprendido entre 128 y 191, incluyendo ambos. En este caso el identificador de la red se obtiene de los dos primeros bytes de la dirección, teniendo que ser un valor entre 128.1 y 191.254 (no es posible utilizar los valores 0 y 255 por tener un significado especial). Los dos últimos bytes de la dirección constituyen el identificador del host permitiendo, por consiguiente, un número máximo de 64516 computadores en la misma red. Este tipo de direcciones tendría que ser suficiente para la gran mayoría de las organizaciones grandes. En caso de que el número de computadores que se necesita conectar fuese mayor, sería posible obtener más de una dirección de "clase B", evitando de esta forma el uso de una de "clase A".

Clase C: En este caso el valor del primer byte tendrá que estar comprendido entre 192 y 223, incluyendo ambos valores. Este tercer tipo de direcciones utiliza los tres primeros bytes para el número de la red, con un rango desde 192.1.1 hasta 223.254.254. De esta manera queda libre un byte para el host, lo que permite que se conecten un máximo de 254 en cada red. Estas direcciones permiten un menor número de host que las anteriores, aunque son las más numerosas pudiendo existir un gran número redes de este tipo (más de dos millones).

Clase	Rango campo red	Rango campo host
Clase A	0 – 127	0.0.0 hasta 255.255.255
Clase B	128.0 hasta 191.255	0.0 hasta 255.255
Clase C	192.0.0 hasta 223.255.255	0 hasta 255
Clase D	224.0.0.0 hasta 239.255.255.255	No aplica
Clase E	240.0.0.0 hasta 247.255.255.255	No aplica

Tabla 1.2 : Tabla de clases de red[8]

En la clasificación de direcciones anterior se puede notar que ciertos números no se usan. Algunos de ellos se encuentran reservados para un posible uso futuro, como es el caso de las direcciones cuyo primer byte sea superior a 223 (clases D y E, que aún no están definidas), mientras que el valor 127 en el primer byte se utiliza en algunos sistemas para propósitos especiales. También es importante notar que los valores 0 y 255 en cualquier byte de la dirección no pueden usarse normalmente por tener otros propósitos específicos. El número 0 está reservado para las máquinas que no conocen su dirección, pudiendo utilizarse tanto en la identificación de red para máquinas que aún no conocen el número de red a la que se encuentran

[8] www.cybercursos.net/tcp-ip.htm

conectadas, en la identificación de host para máquinas que aún no conocen su número de host dentro de la red, o en ambos casos.

El número 255 tiene también un significado especial, puesto que se reserva para el broadcast. El broadcast es necesario cuando se pretende hacer que un mensaje sea visible para todos los sistemas conectados a la misma red. Esto puede ser útil si se necesita enviar el mismo datagrama a un número determinado de clientes, resultando más eficiente que enviar la misma información solicitada de manera individual a cada uno. Otra situación para el uso de broadcast es cuando se quiere convertir el nombre por dominio de un computador a su correspondiente número IP y no se conoce la dirección del servidor de nombres de dominio más cercano.

Lo usual es que cuando se quiere hacer uso del broadcast se utilice una dirección compuesta por el identificador normal de la red y por el número 255 (todo unos en binario) en cada byte que identifique al host. Sin embargo, por conveniencia también se permite el uso del número 255.255.255.255 con la misma finalidad, de forma que resulte más simple referirse a todos los sistemas de la red.

1.12.1.- SISTEMA DE NOMBRES POR DOMINIO (DNS)

El sistema de nombres por dominio (DNS, Domain Name System) es una forma alternativa de identificar a una máquina conectada a Internet. La dirección IP resulta difícil de memorizar, siendo su uso más adecuado para los computadores.

El sistema de nombres por dominio es el utilizado normalmente por las personas para referirse a un computador en la red, ya que además puede proporcionar una idea del propósito o la localización del mismo.

El nombre por dominio de un computador se representa de forma jerárquica con varios nombres separados por puntos.

Para que una máquina pueda establecer conexión es necesario que conozca su número IP, por lo tanto, el nombre por dominio debe ser convertido a su

correspondiente dirección a través de la correspondiente base de datos utilizando los servidores de nombres por dominio (DNS servers). Que son sistemas que contienen bases de datos con el nombre y la dirección de otros sistemas en la red de una forma encadenada o jerárquica

1.12.2.- ENRUTAMIENTO DEL PROTOCOLO

El proceso de enrutamiento de un paquete IP puede ser generalizado por el siguiente algoritmo de enrutamiento:

1. Determinar la dirección IP del computador destino.
2. ¿La red de la dirección IP destino es igual a la red de la dirección IP del computador fuente? Si la respuesta es sí ir al paso 3 de lo contrario ir al paso 4.
3. Obtener la dirección física asociada a la dirección IP destino haciendo uso del protocolo ARP y transmitir el paquete con la interfase de red apropiada.
4-. ¿La red destino se encuentra listada en la tabla de rutas? Si la respuesta es sí enviar el paquete IP a la dirección IP asociada a la ruta hasta alcanzar a la red del computador destino y proceder con el paso 3.. Si la respuesta es no, utilizar la ruta por defecto. Si la ruta por defecto no está configurada: generar un paquete ICMP indicando el error "red inalcanzable".

Durante el proceso de enrutamiento, un paquete IP puede ser fragmentado cuando el tamaño del mismo es mayor que la máxima unidad de transferencia de datos (MTU Maximun Transfer Unit) del enlace que une a dos redes TCP-IP. Los paquetes IP fragmentados sólo son reensamblados cuando llegan al computador destino.

Debido a que el protocolo IP es un protocolo no orientado a conexión[9] el mismo hace uso de un mecanismo que determina el tiempo de vida "TTL Time to Live" de un paquete IP. Este tiempo de vida fijado por el computador Origen es reducido a

[9] Que cada trama en la que ha sido dividido un paquete es tratado por independiente. Las tramas que componen un paquete pueden ser enviadas por caminos distintos e incluso llegar desordenadas.

uno cada vez que el paquete IP es enrutado. Si el tiempo de vida se reduce a cero antes de que el paquete IP llegue a su destino, el paquete IP es destruido.

1.13.- LIMITACIONES DE IPV4

Las limitaciones de IPv4 y que podrán ser solucionadas con la nueva versión son entre otras:

- Escasez de Direcciones: Ya que IPV4 cuenta con un espacio de Direcciones de 32 bits.
- Demasiados sistemas conectados
- Demasiadas entradas en la tabla de ruteo
- Incremento progresivo del tiempo de búsqueda de DNS, etc.
- Nuevas aplicaciones, tales como audio y video, necesitan QoS, Se necesita una nueva arquitectura con mayor flexibilidad topológica, capaz de afrontar el reto que supone la movilidad de sus usuarios.
- Son necesarios esquemas de autenticación y privacidad, tanto para proteger a los usuarios en sí, como la misma integridad de la red ante ataques malintencionados o errores.

1.14.- MOTIVOS DE IPV6

El motivo básico por el que surge es la necesidad de crear un nuevo protocolo, que en un primer momento se denominó IPng (Internet Protocol Next Generation, o “Siguiente Generación del Protocolo Internet”), fue la evidencia de la falta de direcciones.

IPv4 tiene un espacio de direcciones de 32 bits, es decir, hay 4.294.967.296 direcciones. En cambio, IPv6 nos ofrece un espacio exactamente de 340.282.366.920.938.463.463.374.607.431.768.211.456.

Sin embargo, IPv4 tiene otros problemas o “dificultades” que IPv6 soluciona o mejora; Los creadores de IPv4, no predijeron en ningún momento, el gran éxito

que este protocolo iba a tener en muy poco tiempo, en una gran multitud de campos, no sólo científicos y de educación, sino también en innumerables facetas de la vida cotidiana.

Las Tecnologías de la Información han evolucionado de un modo mucho más explosivo de lo esperado. Desde ese momento, y debido a la multitud de nuevas aplicaciones en las que IPv4 ha sido utilizado, ha sido necesario crear "añadidos" al protocolo básico; Entre los "parches" más conocidos, podemos citar medidas para permitir la Calidad de Servicio (QoS [10]), Seguridad (IPsec[11]), y Movilidad[12], fundamentalmente.

Ha sido necesaria la creación de "añadidos/parches" al protocolo básico IPv4. Utilizar cualquiera de los parches es fácil, pero si se pretende usar más de uno conjuntamente, la tarea se complica y se convierte en casi imposible.

1.15.- BREVE RESEÑA HISTÓRICA DEL PROTOCOLO IPV6

Básicamente ha habido tres fases importantes en el desarrollo de IPv4 hasta lo que hoy conocemos como IPv6:

- 1.992 – TUBA
  - √ Implementación de mecanismos para usar TCP y UDP sobre mayores direcciones.
  - √ Se emplea ISO CLNP (Connection-Less Network Protocol, "protocolo de redes sin conexión").
  - √ Se descarta.

[10] Quality Service: Característica del nuevo protocolo IPv6.
[11] Seguridad: característica del nuevo protocolo.
[12] Movilidad: característica del nuevo protocolo.

- 1.993 – SIPP
    - √ Proyecto “Simple IP Plus”.
    - √ Mezcla de SIP y PIP (dos tentativas anteriores para sustituir IPv4).
    - √ Direcciones de 64 bits.

- 1.994 – Ipng
    - √ Se cambia el tamaño de las direcciones a 128 bits.
    - √ Se renombra como IPv6.

Como fase adicional, muy significativa, podemos añadir la constitución oficial, en Julio de 1.999, del “IPv6 Forum” o Foro IPv6, promoción, uso y aplicación del protocolo.

1.16.- CARACTERÍSTICAS DE IPV6

Entre las principales características a mencionar sobre de IPv6 tenemos:

Mayor espacio de direcciones: El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar mas niveles de jerarquías de direccionamiento y mas nodos direccionables; Además soluciona el agotamiento de direcciones IPv4, como el NAT[13], no serian necesarios. Debemos decir que una desventaja de esta nueva dirección es su dificultad para recordarlas dado su tamaño:

[13] **T**raducción de **D**irecciones de **R**edes. NAT hace referencia al proceso de conversión de las direcciones IP utilizadas en una red privada a direcciones IP de Internet

16.16.16.16.16.16.16.16
FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
XXXX.XXXX.XXXX.XXXX.XXXX.XXXX.XXXX.XXXX
8 grupos de 16 bits (en valor hexadecimal) **total de direcciones= 3.402823669 e38** **dirección de 128 bit**

Tabla 1.3: Representación de las direcciones IPv6[14]

Si en una dirección hay 0000 (ceros) se simplifica con un simple 0 ya que no es necesario escribir todos los ceros a la izquierda. Cuando 2 o más campos consecutivos están llenos de 0's (ceros) se puede simplificar de la siguiente manera:

:0000:0000:0000: = :0:0:0:

Esta regla se usa cuando los campos con valor = 0 sean consecutivos y solo una vez se puede usar :: en una direccion ip: por ejemplo:

2002:0450:0009:0010:0000:0000:0000:0071 = 2002:450:9:10::71

FFFF:0:0:0:FFFF:0:0:0 solamente se podrá comprimir en FFFF::FFFF:0:0:0 ó en FFF:0:0:0:FFFF:: pero nunca EN FFFF::FFFF::

Si se encontrara así :: en una dirección, para conocer la dirección completa simplemente se llenan los campos faltantes con 0's hasta completar la dirección de 8 campos: Ejemplos:

[14] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

FFFF::12	**FFFF:0000:0000:0000:0000:0000:0000:0012**
::5	**0000:0000:0000:0000:0000:0000:0000:0005**
1080::8:800:200C:417A	**1080:0000:0000:0000:0008:0800:200C:417A**
1::1	**0001:0000:0000:0000:0000:0000:0000:0001**

Figura1.7: Representación de direcciones IPv6[15]

Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Aggregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits mas bajos son seteados con la dirección MAC (en formato EUI-64). En este caso, el largo del prefijo de la subred es 64, por lo que no hay que preocuparse más por la máscara de red. Además el largo del prefijo no depende en el número de los hosts por lo tanto la asignación es mas simple.

Simplificación del formato del Header. Algunos campos del header IPv4 se quitan o se hacen opcionales

Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits y con una cabecera de longitud fija, más simple, que agiliza su procesado por parte del router.

Posibilidad de paquetes con carga útil (datos) de más de 65.355 bytes.

Seguridad en el núcleo del protocolo (IPsec). El soporte de IPsec es un requerimiento del protocolo IPv6.

[15] http://ditec.um.es/laso/docs/tut-tcpip/3376c216.html

Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flor) de tráfico particular, que requieren manejo especial por los routers IPv6, tal como calidad de servicio no por defecto o servicios de tiempo real. Por ejemplo video conferencia.

Renumeración y "multihoming": facilitando el cambio de proveedor de servicios.

Características de movilidad, la posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad.

Ruteo más eficiente en el backbone de la red, debido a la jerarquía de direccionamiento basada en aggregation.

Calidad de servicio (QoS) y clase de servicio (CoS), Capacidades de autenticación y privacidad

1.17.- VENTAJAS DE IPV6

Entre las principales ventajas podemos mencionar:

Posibilidades extendidas de direccionamiento y de routing. El tamaño de la dirección IP aumenta de 32 a 128 bits, para poder soportar un número más grande de nodos direccionables, más nivel de direcciones jerárquicas y una auto configuración más sencilla de las direcciones.

Un formato de cabecera simplificado y flexible. Algunos campos de formato de la cabecera han sido suprimidos o convertidos en opciones, y la cabecera está simplificada y reducida a una tratamiento común en todos los routers, lo que disminuye el coste del tratamiento en los routers.

Posibilidades de extensión de las cabeceras y de opciones. En IPv6, las opciones están contenidas en cabeceras suplementarias colocadas entre la cabecera IPv6 y

la cabecera del paquete de transporte. La mayoría de las opciones de la cabecera IPv6 no son examinadas ni tratadas por los routers intermedios. Contrariamente a IPv4, las opciones pueden ser de longitud variable, no existe tamaño límite.

Posibilidad de autenticación y de confidencialidad. Ipv6 define extensiones que permiten la autenticación de los usuarios y la integridad de los datos mediante herramientas de criptografía.

Posibilidad de autoconfiguración, Posibilidad para el Source Route. Ipv6 tiene una función extendida de Source Routing gracias a SRDP (Source Demand Routing Protocol) para difundir el routing a rutas interdominio e intradominio.

Posibilidad de calidad de servicio. La introducción de flujos etiquetados (con prioridad) y los servicios de restricciones de tiempo real con nuevos elementos que permiten una mejora en la calidad de servicio.

1.18.- IPV6 EN EL MUNDO Y LATINOAMÉRICA

En el mundo los proyectos de Ipv6 han permitido crear una red mundial experimental en la que se puede probar los conceptos e implementaciones de IPv6. Esta red en su mayor parte esta compuesta por “islas” que soportan IPv6, unidas por enlaces punto a punto llamados “túneles”. En el mundo tenemos un total de 1064 sitios registrados al 6bone en el mundo con 57 países.

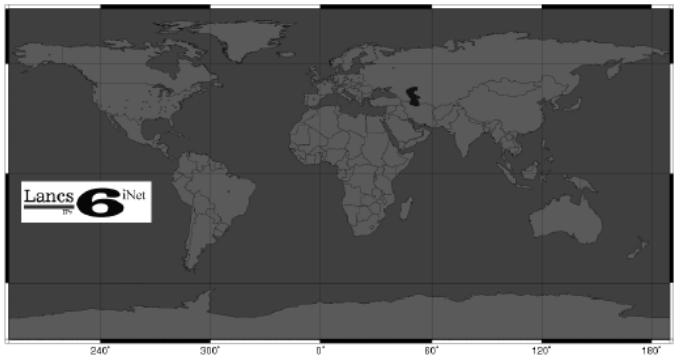


Figura 1.2: Stuación de IPv6 a nivel mundial[16]

Los principales proyectos que a nivel mundial se están desarrollando son:

6Bone

Este es proyecto esta conformado por una red a nivel mundial, que posee las siguientes características:

- √ 1092 nodos, 57 paises, 5 continente.
- √ 116 nodos de Backbone: Esnet, Cisco, Digital, Bay, 3Com, Cairn, Merit, ATT, vBNS, Sprint, Abilene, 6TAP, UNAM, etc.

6REM

Este proyecto es pensado como una red IPv6 para investigaciones y educación, posee las siguientes características:

- √ Red de producción
- √ Enlaces IPv6 nativos y ATM.
- √ ESnet, Internet 2/vBNS, Canarie, Cairn y WIDE

6TAP

Proyecto patrocinado por Canarie y Esnet para dar servicios de ruteo con IPv6

[16] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

IPV6 FORUM

Es un consorcio mundial de fabricantes e instituciones (+100 miembros), cuya finalidad es promover el desarrollo, instalación y uso de IPv6 y sus aplicaciones.
En América Latina podemos decir que en los actuales momentos contamos con 53 sitios en total repartidos de la siguiente manera:

Argentina (12), Brasil (12), Chile (3), Colombia (4), Cuba (1), R. Dominicana (3), México (15), Perú (2), Uruguay (1).

Figura 1.3 Distribución nodos IPv6 en América Latina[17]

1.19.- IPV6 EN ECUADOR

En Ecuador, actualmente no se ha explotado todavía esta tecnología talvez por falta de conocimiento, información o por no ser todavía necesaria su aplicación,

[17] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

pero en un determinado momento se necesitará hacer uso de está, debido a que la tecnología crece a pasos agigantados y es indispensable hacer uso de ella.

En cuanto a los proveedores servicios de Internet, todavía no se encuentran preparados tecnológicamente para recibir a este nuevo protocolo; pero en un futuro cercano tienen planes de implementar y ofrecer conexiones bajo IPv6.

Las instituciones educativas tales como Universidades y Escuelas Politécnicas se encuentran en la obligación de promocionar y proporcionar información para que Ecuador adopte IPv6 como parte de su tecnología.

1.20.- IPV6 EN LA ESPEL

La ESPE-L al momento emplea la tecnología IPv4 y en cuanto a lo que es IPv6 solo se a tenido escasos conocimientos dado a que esta tecnología no se utiliza ni se a difundido todavía dentro del país.

El propósito es aportar toda la información posible de lo que es IPv6, las ventajas y desventajas al utilizarlo y un mecanismo de migración desde IPv4 a IPv6 para que en el momento que esta tecnología llegue al Ecuador la ESPEL ya este preparada para migrar.

Además se puede aportar como fuente de información para otras instituciones que deseen informarse acerca se esta nueva tecnología.

1.21.- EL PROTOCOLO IPV6

Hasta el día de hoy la red Internet funciona gracias a un protocolo general para redes de computadores llamado TCP/IP (*Transfer Control Protocol/Internet Protocol*), en concreto la versión 4, o IPv4.

El protocolo IPv4 empieza a mostrar signos de debilidad. El más importante es la escasez de direcciones IP libres. No obstante la solución ya está preparada y en camino en forma de una nueva versión.

La organización conocida como IETF (*Internet Engineering Task Force*, Comando de Ingeniería de Internet) ha desarrollado un nuevo protocolo llamado IP Next Generation, IPng o IPv6, que soluciona el problema de la limitación de direcciones y mejora otros aspectos técnicos como en enrutamiento y la autoconfiguración. IPv6 es el siguiente paso a IPv4 ya que soluciona muchos problemas.

1.22.- FORMATO DE LA CABECERA IPV6

El tamaño de la cabecera que el protocolo IPv6 añade a los datos es de 320 bits, el doble que en la versión 4. Sin embargo, esta nueva cabecera se ha simplificado con respecto a la anterior. Algunos campos se han retirado, mientras que otros se han convertido en opcionales por medio de las extensiones. De esta manera no se tendrá que procesar parte de la información de la cabecera, lo que permite aumentar de rendimiento en la transmisión. El formato completo de la cabecera sin las extensiones es el siguiente; pero antes observaremos el formato de IPv4

Bits	4	8	16	20	32
Versión	Cabecera	TOS	Longitud Total		
Identificación			Indicador	Desplazamiento de Fragmentación	
TTL		Protocolo	Checksum		
Dirección Fuente 32 bits					
Dirección Destino 32 bits					

Opción

Figura 1.4: Cabecera de IPv4[18]

Campo Modificado
Campo que Desaparece

Figura 1.5 : Campos Modificados y que Desaparecen[19]

En la tabla anterior, se encuentra marcado, mediante el color de fondo, los campos que van a desaparecer en IPv6, y los que son modificados.

Se a pasado de tener 12 campos en IPv4, a tan solo 8 en IPv6. El motivo fundamental por el que los campos eliminados son innecesarios y redundantes. En IPv4 estamos facilitando la misma información de varias formas. Un caso muy evidente es el checksum o verificación de la integridad de la cabecera: Otros mecanismos de encapsulado ya realizan esta función (IEEE 802) MAC.

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

- Algunos de los campos son renombrados:

[18] http://long.ccaba.upc.es/long/050Dissemination_Activities/carlos_ralli_transitiontutorial.pdf
[19] http://long.ccaba.upc.es/long/050Dissemination_Activities/carlos_ralli_transitiontutorial.pdf

Longitud total: longitud de carga útil (payload length), que en definitiva, es la longitud de los propios datos, y puede ser de hasta 65.536 bytes. Tiene una longitud de 16 bits (2 bytes).

Protocolo: siguiente cabecera (next header), dado que en lugar de usar cabeceras de longitud variables se emplean sucesivas cabeceras encadenadas, de ahí que desaparezca el campo de opciones. En muchos casos ni siquiera es procesado por los encaminadores, sino tan sólo extremo a extremo. Tiene una longitud de 8 bits (1 byte).

Tiempo de vida: límite de saltos (Hop Limit). Tiene una longitud de 8 bits (1 byte).

- Los nuevos campos son:

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

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

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

Bit**s** **4** **12** **16** **24**
32

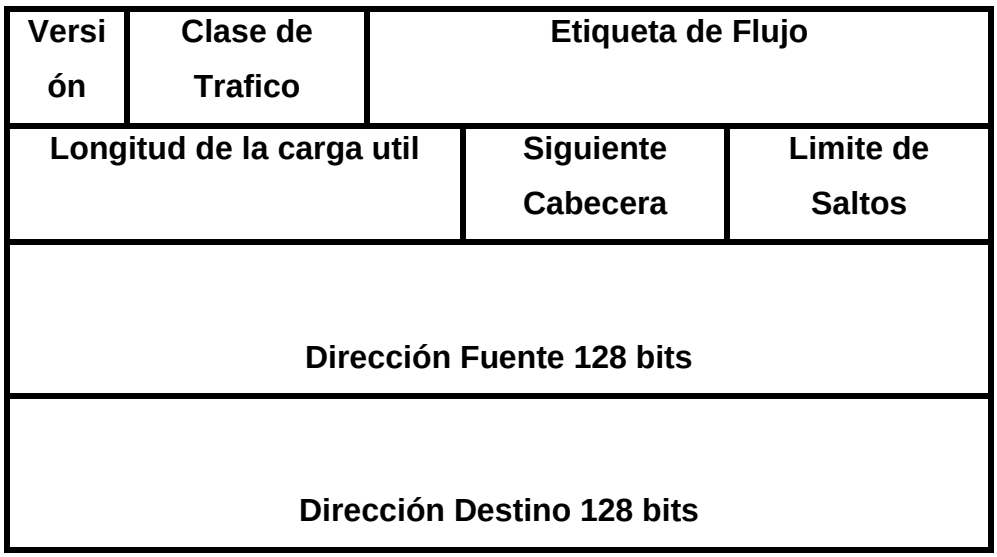


Figura 1.6: Cabecera IPv6[20]

- **Versión:** Número de versión del protocolo IP, que en este caso contendrá el valor 6. *Tamaño: 4 bit.*
- **Prioridad:** Contiene el valor de la prioridad o importancia del paquete que se está enviando con respecto a otros paquetes provenientes de la misma fuente. *Tamaño: 4 bit.*
- **Etiqueta de flujo:** Campo que se utiliza para indicar que el paquete requiere un tratamiento especial por parte de los *routers* que lo soporten. *Tamaño: 24 bit.*

[20] http://long.ccaba.upc.es/long/050Dissemination_Activities/carlos_ralli_transitiontutorial.pdf

- **Longitud:** Es la longitud en bytes de los datos que se encuentran a continuación de la cabecera. *Tamaño: 16 bit.*
- **Siguiente cabecera:** Se utiliza para indicar el protocolo al que corresponde la cabecera que se sitúa a continuación de la actual. El valor de este campo es el mismo que el protocolo en la versión 4 de IP. *Tamaño: 8 bit.*
- **Límite de existencia:** Tiene el mismo propósito que el campo de la versión 4, y es un valor que disminuye en una unidad cada vez que el paquete pasa por un nodo. *Tamaño:8 bit.*
- **Dirección de origen:** El número de dirección del *host* que envía el paquete. Su longitud es cuatro veces mayor que en la versión 4. *Tamaño: 128 bit.*
- **Dirección de destino:** Número de dirección de destino, aunque puede no coincidir con la dirección del *host* final en algunos casos. Su longitud es cuatro veces mayor que en la versión 4 del protocolo IP. *Tamaño: 128 bit.*

Las extensiones que permite añadir esta versión del protocolo se sitúan inmediatamente después de la cabecera normal, y antes de la cabecera que incluye el protocolo de nivel de transporte. Los datos situados en cabeceras opcionales se procesan sólo cuando el mensaje llega a su destino final, lo que supone una mejora en el rendimiento. Otra ventaja adicional es que el tamaño de la cabecera no está limitado a un valor fijo de bytes como ocurría en la versión 4.

Por razones de eficiencia, las extensiones de la cabecera siempre tienen un tamaño múltiplo de 8 bytes. Actualmente se encuentran definidas extensiones para *routing* extendido, fragmentación y ensamblaje, seguridad, confidencialidad de datos, etc.

1.23.- CABECERA DE EXTENSIÓN IPV6

En IPv6, la información opcional de la capa de Internet se codifica en cabeceras separadas se han de colocar en un paquete entre la cabecera de IPv6 y las cabeceras de capas superiores. Existen un número pequeño de tales cabeceras de extensión, cada una identificada por un valor distintivo en el campo “Next Header”

(siguiente cabecera). Como se ilustra en los siguientes ejemplos, un paquete de IPv6 puede llevar cero, una o más cabeceras de extensión, cada una identificada por el campo “Next Header” (sigiente cabecera) de la cabecera anterior:

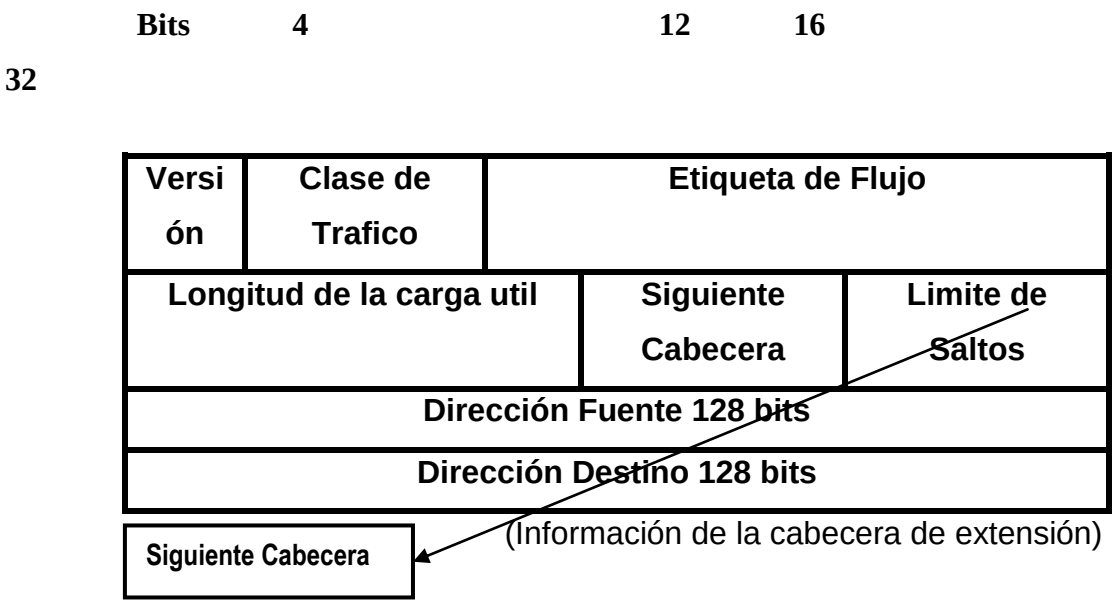


Figura 1.7: Paquete Ipv6 con Cabecera de Extensión[21]

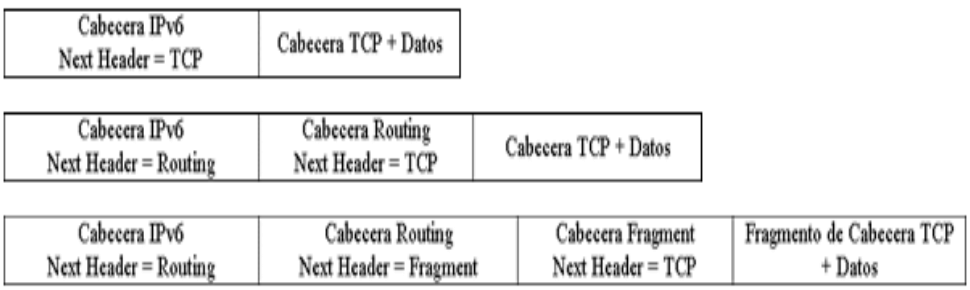


Figura 1.14: Cabeceras de Extensión[22]

[21] http://long.ccaba.upc.es/long/050Dissemination_Activities/carlos_ralli_transitiontutorial.pdf

[22] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

Con una excepción, las cabeceras no son examinadas ni procesadas por ningún nodo a lo largo de la ruta de entrega del paquete, hasta que el paquete alcanza el nodo (o cada uno del conjunto de nodos en el caso del multienvío) identificado en el campo Destination address (campo destino) de la cabecera IPv6. Una vez allí el demultiplexado normal de la cabecera Next Header (cabecera siguiente) invoca al modulo para procesar la primera cabecera de extensión o las cabeceras de las capas superiores si no existe ninguna cabecera de extensión.

El contenido y la semántica de cada cabecera de extensión determinan o no el proceso de la cabecera siguiente. Por lo tanto, las cabeceras de extensión se deben procesar estrictamente en el orden que aparecen en el paquete; un receptor no debe, por ejemplo, examinar un paquete buscando un tipo particular de cabecera de extensión y procesar esa cabecera antes de procesar todas las precedentes.

La excepción mencionada en el párrafo anterior es la Cabecera de Opciones de Hop-by-Hop (Salto a Salto), la cual lleva información que debe ser examinada y procesada por cada nodo a lo largo de la ruta de envío de un paquete, incluyendo los nodos de origen y de destino. La Cabecera de Opciones Hop-by-Hop, cuando está presente, debe seguir inmediatamente a la cabecera IPv6. Su presencia se indica con el valor cero en el campo Next Header de la cabecera IPv6.

Si, como resultado de procesar una cabecera, un nodo necesita proceder a la cabecera siguiente pero el valor Cabecera Siguiente en la cabecera actual es desconocido por el nodo, debe descartar el paquete y enviar un mensaje ICMP[23] de Problema de Parámetro al origen del paquete, con un valor Código ICMP de 1 ("encontrado tipo de Cabecera Siguiente desconocido") y el campo Puntero ICMP conteniendo el desplazamiento del valor desconocido dentro del paquete original. La

[23] (*Internet Control Message Protocol*) proporciona información de control sobre la capa IP; informar posibles errores IP que puedan surgir a lo largo del tránsito de un datagrama.

misma acción se debería tomar si un nodo encuentra un valor Next Header de cero en cualquier cabecera con excepción de una cabecera IPv6.

Cada cabecera de extensión es un entero múltiplo de 8 octetos de longitud, para conservar la alineación de 8 octetos para las cabeceras subsiguientes. Los campos Multi-octeto dentro de cada cabecera de extensión se alinean en sus límites naturales, es decir, campos con un ancho de n octetos son colocados en un entero múltiplo de n octetos desde el inicio de la cabecera, para n = 1, 2, 4, o 8.

Una implementación completa del IPv6 comprende la implementación de las siguientes cabeceras de extensión:

- Hop-by-Hop options, opciones salto a salto.
- Routing, enrutado.
- Fragment, fragmento.
- Destination Options, opciones de destino.
- Authentication, Autenticación.
- Encapsulating Security Payload, Seguridad del Encapsulado de la Carga Útil

1.23.1.- ORDEN DE LAS CABECERAS DE EXTENSIÓN

Cuando se usan más de una cabecera de extensión en un mismo paquete, se recomienda que aparezcan en el siguiente orden:

- Cabecera IPv6.
- Cabecera de opción “Hop-by-Hop”.
- Cabecera de Opción “Destination” (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 Routing).
- Cabecera “Routing”. (enrutamiento)

- Cabecera “Fragment”. (Fragmento)
- Cabecera “Authentication”. (autenticación)
- Cabecera “Encapsulatig Security Payload”. (seguridad del encapsulado de la carga util)
- Cabecera de opción “Destination”(para las opciones a ser procesadas solo por el destino final del paquete).
- Cabecera de la capa superior.

Cada cabecera de extensión debe aparecer como mucho una sola vez, salvo la cabecera de opción “destination”, que puede aparecer como mucho dos veces (una antes de la cabecera “routing” y otra antes de la cabecera de la capa superior).

Si la cabecera de la capa superior es otra cabecera IPv6 (en el caso de que el IPv6 sea tunelizado o encapsulado en IPv6), puede seguirse de sus propias cabeceras de extensión.

Siempre y cuando se definan otras cabeceras de extensión, se ha de especificar el orden con respecto a la lista arriba indicada .

Los nodos IPv6 deben aceptar e intentar procesar cabeceras de extensión en cualquier orden y cualquier número de veces que aparezcan en un mismo paquete, a excepción de la cabecera de Opciones de Hop-by-Hop la cual está restringida a aparecer solamente inmediatamente después de una cabecera IPv6. No obstante, se aconseja imperiosamente que las fuentes de paquetes IPv6 se adhieran al orden recomendado arriba, hasta y a menos que especificaciones subsiguientes corrijan esa recomendación.

1.23.2.- OPCIONES

Las cabeceras “Hop-by-Hop” y “destination” permiten un número variable de opciones codificadas tipo-longitud-valor (TLV), con el siguiente formato:

Tipo de opción	Longitud de datos de la Opción	Datos de la opción

Figura 1.7: Estructura de la cabecera opciones[24]

Tipo de Opción: identificador del tipo de opción de 8 bits.
Longitud de datos de la Opción: Entero sin signo de 8 bits. Es la longitud del campo datos de la opción de esta opción medida en octetos.
Datos de la Opción: Campo de longitud variable. Datos específicos del Tipo de Opción.

La secuencia de opciones dentro de una cabecera se deben procesar estrictamente en el orden que aparecen en la cabecera; un receptor no debe, por ejemplo, examinar a través de una cabecera buscando un tipo en particular de opción y procesar esa opción antes de procesar todas las precedentes.

Los identificadores Tipo de Opción se codifican internamente de modo que sus dos bits de mayor peso especifican la acción que se debe realizar si el nodo IPv6 en proceso no reconoce el Tipo de Opción:

- **00:** saltar la opción y continuar procesando la cabecera.
- **01:** descartar el paquete.
- **10:** descartar el paquete y enviar un ICMP señalando que el tipo de opción es desconocido sin tener en cuenta si la dirección de destino es multienvío o no.
- **11:** descartar el paquete y enviar un ICMP señalando que el tipo de opción es desconocido si la dirección de destino no es multienvío.

[24] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

El tercer bit de mayor peso, indica si los datos específicos de la opción pueden cambiar durante el recorrido del paquete. Esto es útil cuando existe una cabecera de autenticación. Cualquier mecanismo de autenticación deberá tomar como o´s los datos que puedan cambiar en ruta. Los valores son:

- **0:** los Datos de Opción NO cambian el enrutado.
- **1:** los Datos de Opción pueden cambiar el enrutado.

El mismo espacio de numeración de la Tipo de Opción se usa tanto para la cabecera "Hop-by-Hop" como para la cabecera "Destination". Sin embargo, la especificación de una opción en particular puede restringir su uso a solamente una de esas dos cabeceras.

Todo a 1´s	Longitud relleno	Todos a o´s
8 bits	8 bits	(longitud relleno) 2 Octetos

Figura 1.8: Estructura de la cabecera con dos opciones de relleno[25]

Dos de las da las cabeceras de extensión actualmente definidas " cabecera opciones de salto a salto" y la cabecera "opciones de destino" llevan un número variable de "opciones" codificadas tipo longitud_valor (TLV) de la siguiente forma:

Tipo de Opción: Identificador de 8 bits del tipo de opción.
Los datos OPC: Entero sin signo de 8 bits. Longitud del campo datos de la Opción de esta pción, en octetos

[25] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

1.23.3.- CABECECERA OPCIONES DE SALTO A SALTO

La cabecera extendida de *Opciones Salto a Salto* se usa para contener información que deberá ser examinada por cada nodo que encamine el paquete hacia su destino. Este tipo de cabecera se identifica con valor 0 en el campo *siguiente cabecera*. Su formato es el siguiente:

Siguiente cabecera	Longitud opciones	Opciones
8 bits	8 bits	Long. Variable

Figura 1.9: Estructura de la cabecera salto a salto[26]

Siguiente cabecera: Este campo ocupa 1 octeto, e identifica el tipo de cabecera existente inmediatamente después de la de *Opciones Salto a Salto.*
Longitud opciones: Este campo ocupa 1 octeto, e indica la longitud de la cabecera, en octetos, sin incluir los ocho primeros.
Opciones: Este campo es de longitud variable, y contiene opciones del tipo descrito en el punto *Opciones.*

Además de las opciones con la estructura descrita, existe una opción especial, la *Carga Jumbo*. Con la siguiente estructura:

194 (identificador)	4 (long. Opciones)	Longitud Carga Jumbo
8 bits	8 bits	32 bits

Figura 1.10: Estructura de la Carga Jumbo[27]

[26] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

La opción *Carga Jumbo*, es utilizada para enviar paquetes con cargas superiores a los 65535 octetos. La longitud especificada por la *Carga Jumbo* es el tamaño total del paquete, excluyendo la cabecera IPv6, e incluyendo la cabecera de *Opciones Salto a Salto*.

La longitud determinada debe ser siempre superior a 65535, si se recibe un paquete con una *Carga Jumbo* que indique un tamaño de paquete igual o menor a 65535, ICMP se encargará de enviar un error.

Cada paquete cuya longitud esté especificada por un opción *Carga Jumbo*, debe tener a 0 el campo *longitud de la carga* en la cabecera IPv6, además, la opción *Carga Jumbo* no puede ser usada en un paquete conteniendo un fragmento. El incumplimiento de cualquiera de estas restricciones provocara un error ICMP.

1.23.4.- CABECERA DE ENRUTAMIENTO

La Cabecera de Enrutamiento, es utilizada por el remitente para indicar uno o más nodos que el paquete debe visitar en su recorrido. Su formato es el siguiente:

Siguiente cabecera	Longitud cabecera	Tipo enrutamiento	Nodos restantes	Datos
8 bits	8 bits	8 bits	8 bits	Long.Variable

Figura 1.11: Estructura de la cabecera de Enrutamiento[28]

- **Siguiente cabecera:** Este campo ocupa 1 octeto, e identifica el tipo de cabecera siguiente.
- **Longitud cabeceras :** Este campo ocupa 1 octeto, e indica la longitud de la cabecera, en octetos, sin incluir los ocho primeros.

---

[27] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

[28] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

- **Tipo de enrutamiento:** Este campo ocupa 1 octeto, e indica el tipo particular de cabecera de enrutamiento.
- **Nodos restantes:** Este campo ocupa 1 octeto, e indica el número de nodos que restan por visitar, siempre sobre los nodos marcados explícitamente.
- **Datos:** Este campo tiene un longitud variable, siempre múltiplo de 8 (en octetos), y su formato viene determinado por el tipo de enrutamiento específico.

Si un nodo encuentra un paquete con un tipo de enrutamiento desconocido, tomará alguna de estas dos medidas:

√ Si el número de nodos restantes es cero (0), se ignora la cabecera y se pasa a la cabecera siguiente.

√ Si el número de nodos restantes NO es cero, se descarta el paquete y se enviará un error ICMP

El Tipo 0 (*tipo de enrutamiento* = 0) tiene el siguiente formato:

Sig. Cabecera (8 bits)	**Long. Cab. (8 bits)**	**Tipo (= 0) (8 bits)**	**Nodos rest. (8 bits)**	**Reservado (8 bits)**	**Req. vecinos (24 bits)**
Primera Dirección					
"					
[…]					
[…]					
n-ésima Dirección					

Figura1.12: Estructura de la cabecera con tipo de enrutamiento igual a 0[29]

La longitud de la cabecera se especifica en unidades de 8 octetos, sin incluir los 8 primeros octetos, para el Tipo 0, es igual al doble de direcciones especificadas, y

[29] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

debe ser un número par menor o igual a 46, de igual forma, el máximo número de nodos que pueden especificarse es 23.

Existe un campo marcado como *reservado*, el remitente debe ponerlo a cero, y es ignorado por el receptor.

El campo *requerimiento vecinos* (*Strict / Loose Bit Map)* ocupa 24 bits, y es interpretado bit a bit, de izquierda a derecha, para bit, indica si la dirección especificada debe corresponder a un nodo vecino del anterior. 1 significa que el nodo debe ser vecino del anterior, 0 significa que no ha de serlo necesariamente.

Las direcciones a visitar se especifican una tras otra, se numeran de 1 a n y pueden aparecer como máximo 23.

En el Tipo 0 no pueden aparecer direcciones *multicast*. Si un paquete IPv6 tiene como destino una dirección *multicast*[30]*,* no puede contener una cabecera de enrutamiento Tipo 0.

1.23.5.- CABECERA DE FRAGMENTO

La Cabecera de fragmento es utilizada por el origen del paquete IPv6 para enviar paquetes cuyo tamaño excede el mínimo MTU (*Maximum Transmission Unit)* en el camino del paquete. Al contrario que en IPv4, la fragmentación sólo la lleva a cabo el origen. La cabecera tiene el siguiente formato:

Sig. Cabecera	Reservado	Ofsset fragmento	Reservado	flag M	Identificación

[30] Es un mensaje que se envía simultáneamente a un grupo de nodos específicos en una red.

	1		2		
8 bits	**8 bits**	**13 bits**	**2 bits**	**1 bit**	**32 bits**

Figura 1.13: Estructura de la Cabecera Fragmento[31]

Siguiente cabecera: Este campo ocupa 1 octeto, e indica el tipo de la cabecera siguiente.

Reservado 1: Este campo ocupa 1 octeto. El origen lo pone a 0's y es ignorado en destino.

Offset de fragmento: Este campo ocupa 13 bits, e indica, en unidades de 8 octetos, el desplazamiento respecto de la parte fragmentable del paquete original.

Reservado 2: Este campo ocupa 2 bits. El origen lo pone a 0's y es ignorado en destino.

Flag M: Este campo ocupa un bit, es el flag de *más fragmentos*. Si 1, indica que quedan más fragmentos, si 0, indica que es el último fragmento.

Identificación: Este campo ocupa 32 bits, y sirve para identificar los fragmentos pertenecientes al datagrama original.

1.23.6.- CABECERA DE OPCIONES DE DESTINO

Esta cabecera se usa para contener información que sólo debe ser examinada por el nodo destino. La cabecera tiene el siguiente formato :

Siguiente Cabecera	Longitud cabecera	Opciones
8 bits	**8 bits**	**Long. Variable**

Figura 1.14: Estructura de la Cabecera de Opciones de destino[32]

Siguiente Cabecera: Este campo ocupa 1 octeto, e indica el tipo de la cabecera siguiente.

[31] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf
[32] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

Longitud cabecera: Este campo ocupa 1 octeto, e indica la longitud de la cabecera en unidades de 8 octetos, sin incluir los 8 primeros.
Opciones: Este campo tiene una longitud variable, siempre alineada a 8 octetos. Contiene una o más opciones de la estructura

Opciones TLV

Hay dos posibles formas de codificar opciones TLV, como una opción en la cabecera *Opciones en destino*, o como una cabecera extendida aparte. Elegir una forma u otra dependerá de cual sea la acción deseada si el destino no entiende la información.

- Si se quiere que el destino, en caso de no reconocer la opción, descarte el paquete y envíe un error ICMP (sólo si la dirección destino no es *multicast)*. Entonces la opción deberá ser codificada en una cabecera extendida aparte.
- Si se requiere cualquier otra acción, entonces la opción se codificará dentro de una cabecera *Opciones en destino*, y la acción especificada vendrá dada por los dos bit de mayor peso del campo *Tipo de opción*, en la forma descrita en el apartado *Opciones TLV*.

1.23.7.- CABECERA NO HAY SIGUIENTE

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

1.24.- CUESTIONES DEL TAMAÑO DEL PAQUETE

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

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

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

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

Se recomienda fuertemente que los nodos IPv6 implementen el descubrimiento de la MTU de la Ruta con el propósito de descubrir y tomar ventaja de las rutas con MTUs mayores que 128 octetos. Sin embargo, una implementación IPv6 mínima (por ejemplo, en una ROM de inicio) puede restringirse simplemente a enviar paquetes no más grandes que 1280 octetos, y omitir la implementación del descubrimiento de la MTU de la Ruta.

Con el propósito de enviar un paquete más grande que la MTU de la ruta, un nodo puede utilizar la cabecera Fragmento IPv6 para fragmentar el paquete en el origen y tenerlo reensamblado en el(los) destino(s). Sin embargo, el uso de tal fragmentación se desalienta en cualquier aplicación que pueda ajustar sus paquetes para satisfacer la MTU de la ruta medida (es decir, por debajo de los 128 octetos).

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

grandes que 1500 octetos a menos que tenga la certidumbre que el destino es capaz reensamblar paquetes de esos tamaños tan grandes.

En contestación a un paquete IPv6 que se envía a un destino IPv4 (es decir, un paquete que experimenta la traducción del IPv6 al IPv4), el nodo IPv6 originalmente puede recibir un mensaje ICMP Paquete Demasiado Grande reportando de una MTU del Salto Siguiente menor a 1280. En ese caso, no se exige que el nodo IPv6 reduzca el tamaño de los paquetes subsiguientes a menos de 1280, pero debe incluir una cabecera Fragmento en esos paquetes para que el enrutador traductor de IPv6 a IPv4 pueda obtener un valor Identificación apropiado para usar en los fragmentos IPv4 resultantes. Note que esto significa que la carga útil puede tener que ser reducida a 1232 octetos (1280 menos 40 para la cabecera IPv6 y 8 para la cabecera Fragmento), y más pequeña todavía si se usan cabeceras de extensión adicionales.

1.25.- ETIQUETAS DE FLUJO

El campo Etiqueta de Flujo de 20 bits en la cabecera IPv6 puede ser usado por un origen para etiquetar secuencias de paquetes para los cuales solicita un manejo especial por los enrutadores IPv6, tal como la calidad de servicio no estándar o el servicio en "tiempo real".

Este aspecto del IPv6 está, al momento de escribir, todavía experimental y sujeto a cambio conforme los requisitos para dar soporte a flujos en la Internet se vuelvan más claros. Se exige a los hosts o a los enrutadores que no dan soporte a las funciones del campo Etiqueta de Flujo poner el campo a cero al originar un paquete, pasar el campo inalterado al reenviar un paquete, e ignorar el campo al recibir un paquete.

1.26.- CLASES DE TRÁFICO

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

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

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

La interfase 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) especifico de algunos o todos los bits Clase de Tráfico se les permite cambiar el valor de esos bits en los paquetes que ellos originan, reenvían, o reciben, como sea requerido para ese uso específico. Los nodos deben ignorar y dejar sin alterar a 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 son los mimos que el valor enviado por el origen del paquete.

1.27.- PROBLEMAS DEL PROTOCOLO DE CAPA SUPERIOR

1.27.1.- SUMAS DE VERIFICACIÓN DE CAPA SUPERIOR

Cualquier protocolo de transporte u otro de capa superior que incluya las direcciones de la cabecera IP en su cálculo de suma de verificación debe modificarse para el uso sobre el IPv6, para incluir las direcciones IPv6 de 128 bits en lugar de las direcciones IPv4 de 32 bits. En particular, la siguiente ilustración muestra la "pseudos cabecera" TCP y UDP para IPv6:

Dirección Origen	
Dirección Destino	
Longitud del Paquete de Capa Superior	
Cero	Cabecera Siguiente

Figura 1.15: Estructura pseudos cabecera TCP y UDP para IPv6[33]

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

El valor Cabecera Siguiente en la pseudo cabecera identifica el protocolo de capa superior (por ejemplo, 6 para el TCP, o 17 para el UDP). Diferirá del valor Cabecera

[33] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

Siguiente en la cabecera IPv6 si hay cabeceras de extensión entre la cabecera IPv6 y la cabecera de capa superior.

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

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

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

La versión IPv6 del ICPM [ICMPv6] incluye la pseudo cabecera citada arriba en su cálculo de suma de verificación; éste es un cambio a diferencia de la versión IPv4 del ICMP, el cual no incluye unas pseudo cabeceras en su suma de verificación. La razón para el cambio es para proteger al ICMP de una mala entrega o corrupción de aquellos campos de la cabecera IPv6 de los que depende, los qué, a diferencia del IPv4, no son cubiertos por una suma de verificación de la capa Internet. El campo Cabecera Siguiente en la pseudo cabecera para el ICMP contiene el valor 58, que identifica la versión IPv6 del ICMP.

1.27.2.- TIEMPO DE VIDA MÁXIMA DE UN PAQUETE

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

1.27.3.- TAMAÑO MÁXIMO DE LA CARGA ÚTIL DE LA CAPA SUPERIOR

Al calcular el tamaño máximo de carga útil disponible para los datos de capa superior, un protocolo de capa superior debe tener en cuenta el tamaño más grande de la cabecera IPv6 relativo a la cabecera IPv4.

Por ejemplo, en el IPv4, la opción MSS[34] del TCP se calcula como el tamaño máximo de paquete (un valor por defecto o un valor aprendido a través del Descubrimiento de la MTU de la Ruta) menos 40 octetos (20 octetos para la longitud mínima de la cabecera IPv4 y 20 octetos para la longitud mínima de la cabecera TCP). Al usar TCP sobre IPv6, el MSS debe calcularse como el tamaño máximo de paquete menos 60 octetos, puesto que la longitud mínima de la cabecera IPv6 (es decir, una cabecera IPv6 sin cabeceras de extensión) es 20 octetos más larga que la longitud mínima de la cabecera IPv4.

1.27.4.- CONTESTANDO A UN PAQUETE RECIBIDO

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

[34] *Maximum Segment Size* (MSS, tamaño máximo de segmento)

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

- Los paquetes respuesta que no llevan cabeceras Enrutamiento.

- Los paquetes respuesta que llevan cabeceras Enrutamiento que se derivaron invirtiendo la cabecera Enrutamiento del paquete recibido (por ejemplo, una cabecera Enrutamiento proporcionada por configuración local).

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

1.28.- DIRECCIONES Y DIRECCIONAMIENTO EN IPV6

Ya hemos dicho que IPv6 nos aporta, como principio fundamental, un espacio de 2128 direcciones, lo que equivale a 3,40E38

(340.282.366.920.938.463.463.374.607.431.768.211.456).

1.28.1.- DEFINICIÓN DE DIRECCIONES EN IPV6

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

- *Unicast*: Identificador para una única interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. Es el equivalente a las direcciones IPv4 actuales.
- *Anycast*: Identificador para un conjunto de interfaces (típicamente pertenecen a diferentes nodos). Un paquete enviado a una dirección anycast es entregado en una (cualquiera) de las interfaces identificadas con dicha dirección (la más próxima, de acuerdo a las medidas de distancia del protocolo de encaminado). Nos permite crear, por ejemplo, ámbitos de redundancia, de forma que varias máquinas puedan ocuparse del mismo tráfico según una secuencia determinada (por el routing), si la primera "cae".
- *Multicast*: Identificador para un conjunto de interfaces (por lo general pertenecientes a diferentes nodos). Un paquete enviado a una dirección multicast es entregado a todas las interfaces identificadas por dicha dirección.

La misión de este tipo de paquetes es evidente: aplicaciones de retransmisión múltiple (broadcast).

1.28.2.- DIFERENCIAS CON IPV4

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

- No hay direcciones broadcast (su función es sustituida por direcciones multicast).
- Los campos de las direcciones reciben nombres específicos; denominamos "prefijo" a la parte de la dirección hasta el nombre indicado (incluyéndolo).
- Dicho prefijo nos permite conocer donde esta conectada una determinada dirección, es decir, su ruta de encaminado.
- Cualquier campo puede contener sólo ceros o sólo unos, salvo que explícitamente se indique lo contrario.

- Las direcciones IPv6, indistintamente de su tipo (unicast, anycast o multicast), son asignadas a interfaces, no nodos. Dado que cada interfaz pertenece a un único nodo, cualquiera de las direcciones unicast de las interfaces del nodo puede ser empleado para referirse a dicho nodo.
- Todas las interfaces han de tener, al menos, una dirección unicast link-local (enlace local).
- Una única interfaz puede tener también varias direcciones IPv6 de cualquier tipo (unicast, anycast o multicast) o ámbito.
- Una misma dirección o conjunto de direcciones unicast pueden ser asignados a múltiples interfaces físicas, siempre que la implementación trate dichas interfaces, desde el punto de vista de Internet, como una única, lo que permite balanceo de carga entre múltiples dispositivos.
- Al igual que en IPv4, se asocia un prefijo de subred con un enlace, y se pueden asociar múltiples prefijos de subred a un mismo enlace.

1.28.3.- RESERVA DE ESPACIO DE DIRECCIONAMIENTO EN IPV6

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

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

Tabla 1.3: Direcciones reservadas y no asignadas en IPv6[35]

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

Podemos distinguir las direcciones multicast de las unicast por el valor del octeto de mayor orden de la dirección (FF, o 11111111 en binario, indica multicast). En cambio, en el caso de las anycast, no hay ninguna diferencia, sintácticamente hablando, y por tanto, son tomadas del espacio de direcciones unicast.

√ **Direcciones especiales**

Se han definido también las direcciones para usos especiales como:

Dirección de auto-retorno o Loopback (::1) : No ha de ser asignada a una interfaz física; se trata de una interfaz “virtual”, pues se trata de paquetes que no salen de la

[35] http://long.ccaba.upc.es/long/050Dissemination_Activities/carlos_ralli_transitiontutorial.pdf

máquina que los emite; nos permite hacer un bucle para verificar la correcta inicialización del protocolo (dentro de una determinada máquina).

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

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

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

Figura 1.16: Representación de direcciones IPv6 compatibles con IPv4[36]

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

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

Figura 1.17: Representación de direcciones automáticas IPv4 sobre IPv6[37]

[36] http://aula.linux.org.ar/docs/tecnicos/JKoumian-1/JKoumian-1.htm
[37] http://aula.linux.org.ar/docs/tecnicos/JKoumian-1/JKoumian-1.htm

1.28.4.- REPRESENTACIÓN DE LAS DIRECCIONES EN IPV6

La representación de las direcciones IPv6 sigue el siguiente esquema:

a) x:x:x:x:x:x:x:x, donde “x” es un valor hexadecimal de 16 bits, de la porción correspondiente a la dirección IPv6. No es preciso escribir los ceros a la izquierda de cada campo. Ejemplos:

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

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

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

Pueden representarse como:

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

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

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

Pueden representarse como:

::13.1.68.3
::FFFF:129.144.52.38

La representación de los prefijos IPv6 se realiza del siguiente modo:

dirección-IPv6 / longitud-del-prefijo

donde:

- **dirección-IPv6** = una dirección IPv6 en cualquiera de las notaciones válidas

- **longitud-del-prefijo** = valor decimal indicando cuantos bits contiguos de la parte izquierda de la dirección componen el prefijo

Por ejemplo, las representaciones válidas del prefijo de 60 bits

12AB00000000CD3, son:

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

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

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

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

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

1.28.5.- DIRECCIONES UNICAST LOCALES

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

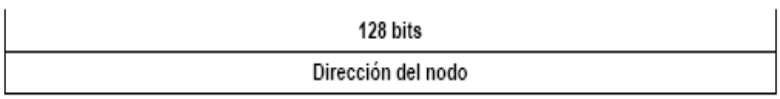


Figura 1.18: Estructura interna de la dirección IPv6 Unicast[38]

[38] http://aula.linux.org.ar/docs/tecnicos/JKoumian-1/JKoumian-1.htm

Un host algo más sofisticado, conocería el prefijo de la subred del enlace al que esta conectado:

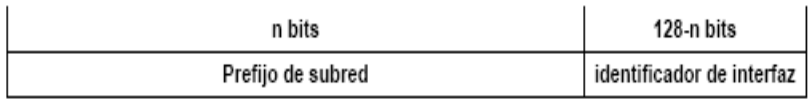


Figura 1.19: Representación de reconocimiento del enlace con dispositivos sofisticados[39]

Dispositivos más sofisticados pueden tener un conocimiento más amplio de la jerarquía de la red, sus límites, etc., en ocasiones dependiendo de la posición misma que el dispositivo o host/router, ocupa en la propia red.

El "identificador de interfaz" se emplea, por tanto, para identificar interfaces en un enlace, y deben de ser únicos en dicho enlace. En muchos casos también serán únicos en un ámbito más amplio. Por lo general, el identificador de interfaz coincidirá con la dirección de la capa de enlace de dicha interfaz. El mismo identificador de interfaz puede ser empleado en múltiples interfaces del mismo nodo, sin afectar a su exclusividad global en el ámbito IPv6.

Se han definido dos tipos de direcciones unicast de uso local: Local de Enlace (Link-Local) y Local de Sitio (Site-Local).

Las direcciones locales de enlace han sido diseñadas para direccionar un único enlace para propósitos de auto-configuración (mediante identificadores de interfaz), descubrimiento del vecindario, o situaciones en las que no hay routers.

[39] http://aula.linux.org.ar/docs/tecnicos/JKoumian-1/JKoumian-1.htm

Por tanto, los encaminadores no pueden retransmitir ningún paquete con direcciones fuente o destino que sean locales de enlace (su ámbito esta limitado a la red local). Tienen el siguiente formato:

10 bits	54 bits	64 bits
1111111010	0	Identificador de interfaz

Figura 1.20: Representación de direcciones locales de enlace[40]

Se trata de direcciones FE80::<ID de interfaz>/10.

Las direcciones locales de sitio permiten direccionar dentro de un "sitio" local u organización, sin la necesidad de un prefijo global. Se configuran mediante un identificador de subred, de 16 bits. Los encaminadores no deben de retransmitir *fuera del sitio* ningún paquete cuya dirección fuente o destino sea "local de sitio" (su ámbito esta limitado a la red local o de la organización).

10 bits	38 bits	16 bits	64 bits
1111111011	0	ID de subred	Identificador de interfaz

Figura 1.21: Representación de direcciones locales de sitio[41]

1.28.6.- DIRECCIONES ANYCAST

Tal y como hemos indicado antes, las direcciones anycast tienen el mismo rango de direcciones que las unicast.

Cuando una dirección unicast es asignada a más de una interfaz, convirtiéndose en una dirección anycast, los nodos a los que dicha dirección ha sido asignada, deben ser explícitamente configurados para que reconozcan que se trata de una

[40] http://aula.linux.org.ar/docs/tecnicos/JKoumian-1/JKoumian-1.htm
[41] http://aula.linux.org.ar/docs/tecnicos/JKoumian-1/JKoumian-1.htm

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

n bits	128-n bits
Prefijo de subred	0000000000000000000

Figura 1.22: Estructura de la dirección ANICAST[42]

Todos los routers han de soportar esta dirección para las subredes a las que están conectados. Los paquetes enviados a la “dirección anycast del router de la subred”, serán enviados a un router de la subred. Una aplicación evidente de esta característica, además de la tolerancia a fallos, es la movilidad. Imaginemos nodos que necesitan comunicarse con un router entre el conjunto de los disponibles en su subred.

Dentro de cada subred, los 128 valores superiores de identificadores de interfaz están reservados para su asignación como direcciones anycast de la subred. La construcción de una dirección reservada de anycast de subred depende del tipo de direcciones IPv6 usadas dentro de la subred. Las direcciones cuyos tres primeros bits (prefijo de formato) tienen valores entre 001 y 111 (excepto las de multicast, 1111 1111), indican con el bit “universal/ local” igual a cero, que el identificador de interfaz tiene 64 bits, y por tanto no es globalmente único (es local). En este caso, las direcciones reservadas anycast de subred se construyen del siguiente modo:

64 bits	57 bits	7 bits
Prefijo de subred	1111110111 ... 111	ID anycast
	Identificador de interfaz	

[42] http://aula.linux.org.ar/docs/tecnicos/JKoumian-1/JKoumian-1.htm

Figura 1.23 : Estructura de la dirección ANICAST con longitud128[43]

En el resto de los casos, el identificador de interfaz puede tener una longitud diferente de 64 bits, por lo que la construcción se realiza según el siguiente esquema:

n bits	121-n bits	7 bits
Prefijo de subred	1111111 ... 1111111	ID anycast
	Identificador de interfaz	

Figura 1.24: Estructura de la dirección ANICAST con longitud 64[44]

1.28.7.- DIRECCIONES MULTICAST

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

Las direcciones multicast tienen el siguiente formato:

8	4	4	112 bits
11111111	000T	ámbito	Identificador de Grupo

Figura 1.25: Estructura de la dirección MULTICAST [45]

El bit “T” indica, si su valor es cero, una dirección multicast permanente, asignada únicamente por la autoridad de numeración global de Internet. En caso contrario, si su valor es uno, se trata de direcciones multicast temporales. Los 4 bits que le preceden, que por el momento están fijados a cero, están reservados para futuras actualizaciones.

---

[43] http://aula.linux.org.ar/docs/tecnicos/JKoumian-1/JKoumian-1.htm
[44] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

[45] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

Los bits “ámbito” tienen los siguientes significados:

0	Reservado
1	Ambito Local de Nodo
2	Ambito Local de Enlace
3	No asignado
4	No asignado
5	Ambito Local de Sitio
6	No asignado
7	No asignado
8	Ambito Local de Organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ambito Global
F	Reservado

Tabla 1.4: Tablas de bits de ámbito[46]

El “Identificador de Grupo”, identifica, como cabe esperar, el grupo de multicast concreto al que nos referimos, bien sea permanente o temporal, dentro de un determinado ámbito.

Por ejemplo, si asignamos una dirección multicast permanente, con el identificador de grupo 101 (hexadecimal), al grupo de los servidores de tiempo (NTS), entonces:

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

[46] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

Las direcciones multicast no-permanentes, sólo tienen sentido en su propio ámbito. Por ejemplo, un grupo identificado por la dirección temporal multicast local de sitio FF15::101, no tiene ninguna relación con un grupo usando la misma dirección en otro sitio, ni con otro grupo temporal que use el mismo identificador de grupo (en otro ámbito), ni con un grupo permanente con el mismo identificador de grupo. Las direcciones multicast no deben ser usadas como dirección fuente en un paquete IPv6, ni aparecer en ninguna cabecera de encaminado. Las principales direcciones multicast reservadas son las incluidas en el rango

FF0x:0:0:0:0:0:0:0.

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

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

La dirección FF02:0:0:0:0:1:FFxx:xxxx, denominada “Solicited-Node Address”,o dirección de nodo solicitada, permite calcular la dirección multicast a partir de la unicast o anycast de un determinado nodo. Para ello, se sustituyen los 24 bits de menor peso (“x”) por los mismos bits de la dirección original. Así, la dirección 4037::01:800:200E:8C6C se convertiría en FF02::1:FF0E:8C6C.

Cada nodo debe de calcular y unirse a todas las direcciones multicast que le corresponden para cada dirección unicast y anycast que tiene asignada.

1.28.8.- DIRECCIONES REQUERIDAS PARA CUALQUIER NODO

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

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

Además, todos los dispositivos con IPv6, deben de tener, predefinidos, los prefijos siguientes:

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

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

1.28.9.- DIRECCIONES UNICAST GLOBALES AGREGABLES

Dado que uno de los problemas que IPv6 resuelve es la mejor organización jerárquica del routing en las redes públicas (globales), es indispensable el concepto de direccionamiento “agregable”.
En la actualidad ya se emplea este tipo de direcciones, basadas en la agregación por parte de los proveedores del troncal Internet, y los mecanismos adoptados para IPv6, permiten su continuidad. Pero además, se incorpora un mecanismo de agregación basado en “intercambios”. La combinación de ambos es la que permite un encaminamiento mucho más eficiente, dando dos opciones de conectividad a unas u otras entidades de agregación. Se trata de una organización basada en tres niveles:

Topología Pública: conjunto de proveedores e “intercambiadores” que proporcionan servicios públicos de tránsito Internet.
Topología de Sitio: redes de organizaciones que no proporcionan servicios públicos de tránsito a nodos fuera de su propio “sitio”.
Identificador de Interfaz: identifican interfaces de enlaces.

En la figura adjunta, el formato de direcciones agregables ha sido diseñado para soportar proveedores de larga distancia (identificados como Proveedor 1-4), intercambiadores (Intercambiador 1 y 2), proveedores de niveles inferiores (podrían ser ISP’s, identificados como Proveedor 5 y 6), y Clientes (Cliente A-F). A diferencia de lo que ocurre actualmente, los intercambiadores también proporcionarán direcciones públicas IPv6. Las organizaciones conectadas a dichos intercambiadores también recibirán servicios de conectividad directos, indirectamente a través del intercambiador, de uno o varios proveedores de larga distancia.

De esta forma, su direccionamiento es independiente de los proveedores de tráfico de larga distancia, y pueden, por tanto, cambiar de proveedor sin necesidad de renumerar su organización. Este es uno de los objetivos de IPv6.

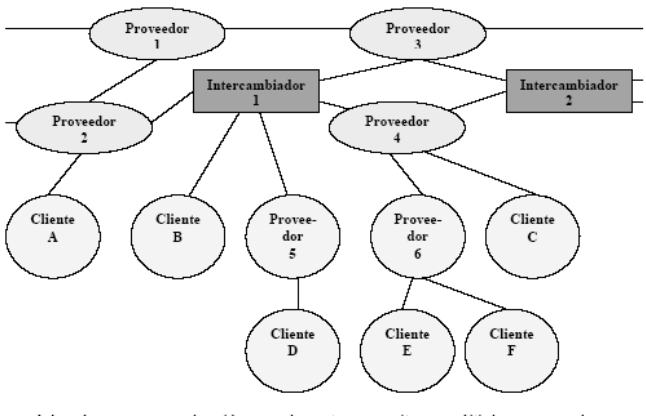


Figura 1.26: Representación de direcciones agregables[47]

Además, una organización puede estar suscrita a múltiples proveedores (multi-homing o "multi-localización"), a través de un intercambiador, sin necesidad de tener prefijos de direcciones de cada uno de los proveedores.

Estructura De Direcciones Unicast Globales Agregables

El formato de las direcciones unicast globales agregables es el siguiente:

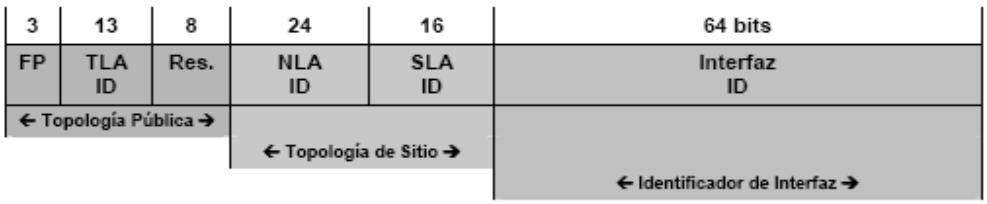


Figura 1.27: Estructura de direcciones unicast globales agregables[48]

[47] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

[48] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

Donde

FP	Prefijo de Formato (001) - Format Prefix
TLA ID	Identificador de Agregación de Nivel Superior - Top-Level Aggregation Identifier
Res.	Reservado para uso futuro
NLA ID	Identificador de Agregación de Siguiente Nivel - Next-Level Aggregation Identifier
SLA ID	Identificador de Agregación de Nivel de Sitio - Site-Level Aggregation Identifier
Interfaz ID	Identificador de Interfaz

Figura 1.28: Especificaciones de campos de las direcciones unicast globales agregables [49]

El campo Reservado permitirá, en el futuro, ampliaciones "organizadas" del protocolo, por ejemplo ampliar el número de bits de los campos TLA y NLA. Por el momento contiene ceros.

Identificador de Agregación de Nivel Superior

Se trata del nivel superior en la estructura jerárquica de enrutado. Los routers situados en este nivel tienen, en la tabla de encaminado, una entrada para cada TLA ID activo, y probablemente entradas adicionales relativas al propio TLA ID donde están físicamente situados. Podrían tener otras entradas, para su optimización, dependiendo de su topología, pero siempre pensando en que se minimice la tabla. Esta estructura de direccionamiento permite 8.192 (213) identificadores de TLA. Se prevé su crecimiento haciendo que este campo crezca hacia la derecha en el espacio reservado para el futuro, o usando este mismo formato/estructura para prefijos de formato (FP) adicionales.

Identificador de Agregación de Siguiente Nivel

[49] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

Es empleado por organizaciones a las que se ha asignado un TLA, para crear una estructura jerárquica de direccionamiento, acorde con su propia red, y para identificar los “sitios” u organizaciones que de ella dependen. Pueden reservar los bits superiores para la diferenciación de la estructura de su red, en función a sus propias necesidades.

n	24-n bits	16	64 bits
NLA1	Site ID	SLA ID	Interfaz ID

Figura 1.29: Estructura con identificador de agregación de siguiente nivel[50]

Dado que cada organización que recibe un TLA (top level agregation) dispone de 24 bits de espacio NLA, permite proporcionar servicio aproximadamente al número total de direcciones IPv4 soportadas actualmente. Las organizaciones que reciben un TLA pueden soportar varios NLA en su propio espacio de direccionamiento (Site ID). Esto permite que sirvan tanto a clientes directos (suscriptores) como a otras organizaciones proveedoras de servicios públicos de tránsito. Y así sucesivamente, como se muestra en la siguiente figura:

n	24-n bits		16	64 bits
NLA1	Site ID		SLA ID	Interfaz ID
	m	24-n-m bits	16	64 bits
	NLA2	Site ID	SLA ID	Interfaz ID
		o 24-n-m-o bits	16	64 bits
		NLA3 Site ID	SLA ID	Interfaz ID

Figura 1.30: Estructura de varios TLA soportando varios NLA [51]

[50] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

[51] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

El diseño del espacio NLA de cada organización es libre para cada TLA asignado, y así sucesivamente con los niveles inferiores. Sin embargo, se recomienda seguir los procedimientos del RFC2050.

En cualquier caso es fundamental apreciar el balance entre eficacia de encaminado agregable y flexibilidad. Las estructuras más jerárquicas permiten una mejor agregación, y por tanto reducen las tablas de encaminado. Por el contrario, asignaciones más planas del espacio NLA proporcionan mejor flexibilidad en la conexión (crecimientos no previstos en un determinado espacio), resultando en tablas de encaminado mayores, y por tanto menos eficaces.

Identificador de Agregación de Nivel de Sitio

El SLA es usado por organizaciones "finales" para crear su propia estructura jerárquica de direcciones e identificar sus subredes. Es equivalente al concepto de subred en IPv4, con la muy apreciable diferencia de que cada corporación tiene un mayor número de subredes (16 bits proporcionan capacidad para 65.535). Del mismo modo que en el caso del NLA, se puede escoger entre una estructura "plana", o crear varios niveles, según la figura adjunta:

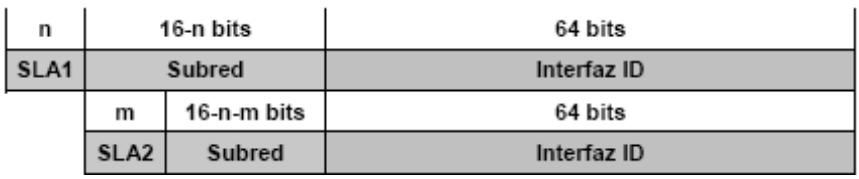


Figura 1.31: Estructura del Identificador de Agregación de Nivel de Sitio[52]

Una gran compañía podría necesitar varios identificadores SLA. Como es lógico, cada caso dependerá de cómo están conectadas sus diversas delegaciones.

[52] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

1.29.- FORMATO PARA LA REPRESENTACION DE URLS

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

La solución es bien sencilla: el empleo de los corchetes **("[","]")** para encerrar la dirección IPv6, dentro de la estructura habitual del URL. Veamos algunos ejemplos; las direcciones siguientes:

- FEDC:BA98:7654:3210:FEDC:BA98:7654:3210
- 1080:0:0:0:8:800:200C:4171
- 3ffe:2a00:100:7031::1
- 1080::8:800:200C:417A
- ::192.9.5.5
- ::FFFF:129.144.52.38
- 2010:836B:4179::836B:4179

Serían representadas como:

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

Hemos añadido alguna “complicación”, para que el propio lector descubra el uso del separador de puertos

1.30.- ICMP VERSIÓN 6

El Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol), descrito originalmente en el documento RFC792 para IPv4, ha sido actualizado para permitir su uso bajo IPv6.

El protocolo resultante de dicha modificación es ICMPv6, y se le ha asignado un valor, para el campo de “siguiente cabecera”, igual a 58. ICMPv6 es parte integral de IPv6 y debe ser totalmente incorporado a cualquier implementación de nodo IPv6. ICMPv6 es empleado por IPv6 para reportar errores que se encuentran durante el procesado de los paquetes, así como para la realización de otras funciones relativas a la capa “Internet”, como diagnósticos (“ping”).

El formato genérico de los mensajes ICMPv6 es el siguiente:

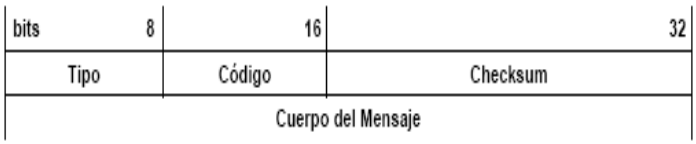


Figura 1.32: Formato de mensajes ICMPv6[53]

El campo "tipo" indica el tipo de mensaje, y su valor determina el formato del resto de la cabecera.

El campo "código" depende del tipo de mensaje, y se emplea para crear un nivel adicional de jerarquía para la clasificación del mensaje.

El checksum o código de redundancia nos permite detectar errores en el mensaje ICMPv6. Los mensajes ICMPv6 se agrupan en dos tipos o clases: mensaje de error y mensajes informativos.

Los mensajes de error tienen cero en el bit de mayor peso del campo "tipo", por lo que sus valores se sitúan entre 0 y 127.

Los valores de los mensajes informativos oscilan entre 128 y 255. Los mensajes definidos por la especificación básica son los siguientes:

[53] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

Mensajes de error ICMPv6		
Tipo	Descripción y Códigos	
1	Destino no alcanzable (Destination Unreachable)	
	Código	Descripción
	0	Sin ruta hacia el destino
	1	Comunicación prohibida administrativamente
	2	Sin asignar
	3	Dirección no alcanzable
	4	Puerto no alcanzable
2	Paquete demasiado grande (Packet Too Big)	
3	Tiempo excedido (Time Exceeded)	
	Código	Descripción
	0	Límite de saltos excedido
	1	Tiempo de desfragmentación excedido
4	Problema de parámetros (Parameter Problem)	
	Código	Descripción
	0	Campo erróneo en cabecera
	1	Tipo de "cabecera siguiente" desconocida
	2	Opción IPv6 desconocida
Mensajes informativos ICMPv6		
Tipo	Descripción	
128	Solicitud de eco (Echo Request)	
129	Respuesta de eco (Echo Reply)	

Tabla 1.5: Tabla de valores de mensajes de error e informativos del ICMP[54]

Se esta trabajando en nuevos tipos de mensajes, siendo el más interesante de ellos el definido en un borrador de IETF (draft-ietf-ipngwg-icmp-name-lookups-05.txt), que permitirá solicitar a un nodo información completa como su "nombre de dominio completamente cualificado" (Fully-Qualified-Domain-Name). Por razones de seguridad, las cabeceras ICMPv6 pueden ser autenticadas y encriptadas, usando la cabecera correspondiente. El uso de este mecanismo permite, además, la prevención de ataques ICMP, como el conocido "Negación de Servicio" (DoS o Denial of Service Attack).

1.31.- NEIGHBOR DISCOVERY

En IPv6, el protocolo equivalente, en cierto modo, a ARP en IPv4, es el que denominamos "descubrimiento del vecindario". Sin embargo, incorpora también la funcionalidad de otros protocolos IPv4, como "ICMP Router Discovery" y "ICMP

[54] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

Redirect". Tal como indica esta "traducción", consiste en el mecanismo por el cual un nodo que se incorpora a una red, descubre la presencia de otros, en su mismo enlace, para determinar sus direcciones en la capa de enlace, para localizar los routers, y para mantener la información de conectividad ("reachability") acerca de las rutas a los "vecinos" activos.

El protocolo ND (abreviatura común de "Neighbor Discovery"), también se emplea para mantener limpios los "caches" donde se almacena la información relativa al contexto de la red a la que esta conectado un nodo (host o router), y por tanto para detectar cualquier cambio en la misma. Cuando un router, o una ruta hacia él, falla, el host buscará alternativas funcionales.

ND emplea los mensajes de ICMPv6, incluso a través de mecanismos de multicast en la capa de enlace, para algunos de sus servicios. El protocolo ND es bastante completo y sofisticado, ya que es la base para permitir el mecanismo de autoconfiguración en IPv6.

Define, entre otros, mecanismos para: descubrir routers, prefijos y parámetros, autoconfiguración de direcciones, resolución de direcciones, determinación del siguiente salto, detección de nodos no alcanzables, detección de direcciones duplicadas o cambios, redirección, balanceo de carga entrante, direcciones anycast, y anunciación de proxies. ND define cinco tipos de paquetes ICMPv6:

Solicitud de Router (Router Solicitation): generado por una interfaz cuando es activada, para pedir a los routers que se "anuncien" inmediatamente.
Tipo en paquete ICMPv6 = 133.

Anunciación de Router (Router Advertisement): generado por los routers periódicamente (entre cada 4 y 1800 segundos) o como consecuencia de una "solicitud de router", a través de multicast, para informar de su presencia así como de otros parámetros de enlace y de Internet, como prefijos (uno o varios), tiempos

de vida, configuración de direcciones, límite de salto sugerido, etc. Es fundamental para permitir la renumeración. Tipo en paquete

ICMPv6 = 134.

Solicitud de Vecino (Neighbor Solicitation): generado por los nodos para determinar la dirección en la capa de enlace de sus vecinos, o para verificar que el nodo vecino sigue activo (es alcanzable), así como para detectar las direcciones duplicadas. Tipo en paquete ICMPv6 = 135.

Anunciación de Vecino (Neighbor Advertisement): generado por los nodos como respuesta a la "solicitud de vecino", o bien para indicar cambios de direcciones en la capa de enlace. Tipo en paquete ICMPv6 = 136.

Redirección (Redirect): generado por los routers para informar a los host de un salto mejor para llegar a un determinado destino. Equivalente, en parte a "ICMP redirect". Tipo en paquete ICMPv6 = 137.

El protocolo ND, frente a los mecanismos existentes en IPv4, reporta numerosas ventajas:

- El descubrimiento de routers es parte de la base del protocolo, no es preciso recurrir a los protocolos de encaminado.
- La anunciación de router incluye las direcciones de la capa de enlace, no es necesario ningún intercambio adicional de paquetes para su resolución.
- La anunciación de router incluye los prefijos para el enlace, por lo que no hay necesidad de un mecanismo adicional para configurar la máscara de red.
- La anunciación de router permite la autoconfiguración de direcciones
- Los routers pueden anunciar a los host del mismo enlace el MTU (tamaño máximo de la unidad de transmisión).

- Se extienden los multicast de resolución de direcciones entre 232 direcciones, reduciendo de forma importante las interrupciones relativas a la resolución de direcciones en nodos distintos al objetivo, y evitando las interrupciones en nodos sin IPv6.
- Las redirecciones contienen la dirección de la capa de enlace del nuevo salto, lo que evita la necesidad de una resolución de dirección adicional.
- Se pueden asignar múltiples prefijos al mismo enlace y por defecto los host aprenden todos los prefijos por la anunciación de router. Sin embargo, los routers pueden ser configurados para omitir parte o todos los prefijos en la anunciación, de forma que los host consideren que los destinos están fuera del enlace; de esta forma, enviarán el tráfico a los routers, quién a su vez lo redireccionará según corresponda.
- A diferencia de IPv4, en IPv6 el receptor de una redirección asume que el siguiente salto esta en el mismo enlace. Se prevé una gran utilidad en el sentido de no ser deseable o posible que los nodos conozcan todos los prefijos de los destinos en el mismo enlace (enlaces sin multidifusión y media compartida).
- La detección de vecinos no alcanzables es parte de la base de mejoras para la robustez en la entrega de paquetes frente a fallos en routers, particiones de enlaces, nodos que cambian sus direcciones, nodos móviles, etc.
- A diferencia de ARP, en ND se puede detectar fallos de la mitad del enlace, es decir, con conectividad en un sólo sentido, evitando el tráfico hacia ellos.
- A diferencia de IPv4, no son precisos campos de preferencia (para definir la “estabilidad” de los routers). La detección de vecinos no alcanzables sustituirá los caminos desde routers con fallos a otros activos.
- El uso de direcciones de enlace local para identificar routers, permite a los hosts que mantengan su asociación con los mismos, en el caso de que se realice una renumeración para usar nuevos prefijos globales.
- El límite de saltos es siempre igual a 255, lo que evita que haya envíos accidentales o intencionados desde nodos fuera del enlace, dado que los routers decrementan automáticamente este campo en cada salto.

- Al realizar la resolución de direcciones en la capa ICMP, se independiza el protocolo del medio, permitiendo mecanismos de autenticación y seguridad normalizados.

En resumen, ND reemplaza, con grandes mejoras e importantes ventajas, a ARP.

1.32.- AUTOCONFIGURACION EN IP6

La autoconfiguración es el conjunto de pasos por los cuales un host decide como autoconfigurar sus interfaces en IPv6. Este mecanismo es el que nos permite afirmar que IPv6 es “Plug & Play”.

El proceso incluye la creación de una dirección de enlace local, verificación de que no esta duplicada en dicho enlace y determinación de la información que ha de ser autoconfigurada (direcciones y otra información).

Las direcciones pueden obtenerse de forma totalmente manual, mediante DHCPv6 (stateful o configuración predeterminada), o de forma automática (stateless o descubrimiento automático, sin intervención).

Este protocolo define el proceso de generar una dirección de enlace local, direcciones globales y locales de sitio, mediante el procedimiento automático (stateless). También define el mecanismo para detectar direcciones duplicadas. La autoconfiguración “stateless” (sin intervención), no requiere ninguna configuración manual del host, configuración mínima (o ninguna) de routers, y no precisa servidores adicionales. Permite a un host generar su propia dirección mediante una combinación de información disponible localmente e información anunciada por los routers. Los routers anuncian los prefijos que identifican la subred (o subredes) asociadas con el enlace, mientras el host genera un “identificador de interfaz”, que identifica de forma única la interfaz en la subred. La dirección se compone por la

combinación de ambos campos. En ausencia de router, el host sólo puede generar la dirección de enlace local, aunque esto es suficiente para permitir la comunicación entre nodos conectados al mismo enlace.

En la autoconfiguración “stateful” (predeterminada), el host obtiene la dirección de la interfaz y/o la información y parámetros de configuración desde un servidor. Los servidores mantienen una base de datos con las direcciones que han sido asignadas a cada host. Ambos tipos de autoconfiguración (stateless y stateful), se complementan. Un host puede usar autoconfiguración sin intervención (stateless), para generar su propia dirección, y obtener el resto de parámetros mediante autoconfiguración predeterminada (stateful).

El mecanismo de autoconfiguración “sin intervención” se emplea cuando no importa la dirección exacta que se asigna a un host, sino tan sólo asegurarse que es única y correctamente enrutable. El mecanismo de autoconfiguración predeterminada, por el contrario, nos asegura que cada host tiene una determinada dirección, asignada manualmente. Cada dirección es cedida a una interfaz durante un tiempo predefinido (posiblemente infinito). Las direcciones tienen asociado un tiempo de vida, que indican durante cuanto tiempo esta vinculada dicha dirección a una determinada interfaz. Cuando el tiempo de vida expira, la vinculación se invalida y la dirección puede ser reasignada a otra interfaz en cualquier punto de Internet.

Para gestionar la expiración de los vínculos, una dirección pasa a través de dos fases diferentes mientras está asignada a una interfaz. Inicialmente, una dirección es “preferred” (preferida), lo que significa que su uso es arbitrario y no está restringido. Posteriormente, la dirección es “deprecated” (desaprobada), en anticipación a que el vínculo con su interfaz actual va a ser anulado. Mientras esta en estado “desaprobado”, su uso es desaconsejado, aunque no prohibido. Cualquier nueva comunicación (por ejemplo, una nueva conexión TCP), debe usar una dirección “preferida”, siempre que sea posible. Una dirección “desaprobada” debería

ser usada tan solo por aquellas aplicaciones que ya la venían utilizando y a las que les es muy difícil cambiar a otra dirección sin interrupción del servicio.

Para asegurarse de que todas las direcciones configuradas son únicas, en un determinado enlace, los nodos ejecutan un algoritmo de detección de direcciones duplicadas, antes de asignarlas a una interfaz. Este algoritmo es ejecutado para todas las direcciones, independientemente de que hayan sido obtenidas mediante autoconfiguración stateless o stateful.

La autoconfiguración esta diseñada para hosts, no para routers, aunque ello no implica que parte de la configuración de los routers también pueda ser realizada automáticamente (generación de direcciones de enlace local). Además, los routers también tienen que “aprobar” el algoritmo de detección de direcciones duplicadas.

1.33.- IPV6 SOBRE ETHERNET

Aunque ya han sido definidos protocolos para permitir el uso de IPv6 sobre cualquier tipo de red o topología (Token Ring, FDDI, ATM), como ejemplo mucho más habitual y básico, centraremos este apartado en Ethernet (CSMA/CD y tecnologías full-duplex.

Los paquetes IPv6 se transmiten sobre tramas normalizadas Ethernet. La cabecera Ethernet contiene las direcciones fuente y destino Ethernet, y el código de tipo Ethernet con el valor hexadecimal 86DD.

El campo de datos contiene la cabecera IPv6 seguida por los propios datos, y probablemente algunos bytes para alineación/relleno, de forma que se alcance el tamaño mínimo de trama para el enlace Ethernet.

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

Figura 1.33: Estructura de la dirección ethernet en IPv6[55]

El tamaño máximo de la unidad de transmisión (MTU), para IPv6 sobre Ethernet, es de 1.500 bytes. Evidentemente, este puede ser reducido, manual o automáticamente (por los mensajes de anunciación de routers).

Para obtener el identificador de interfaz, de una interfaz Ethernet, para la autoconfiguración stateless, nos basamos en la dirección MAC de 48 bits (IEEE802). Tomamos los 3 primeros bytes (los de mayor orden), y les agregamos “FFFE” (hexadecimal), y a continuación, el resto de los bytes de la dirección MAC (3 bytes). El identificador así formado se denomina identificador EUI-64 (Identificador Global de 64 bits), según lo define IEEE. El identificador de interfaz se obtiene, a continuación, partiendo del EUI-64, complementando el bit U/L (Universal/Local). El bit U/L es el siguiente al de menor valor del primer byte del EUI-64 (el 2º bit por la derecha, el 2º bit de menor peso). Al complementar este bit, por lo general cambiará su valor de 0 a 1; dado que se espera que la dirección MAC sea universalmente única, U/L tendrá un valor 0, y por tanto se convertirá en 1 en el identificador de interfaz IPv6.

Una dirección MAC configurada manualmente o por software, no debería ser usada para derivar de ella el identificador de interfaz, pero si no hubiera otra fórmula, su propiedad debe reflejarse en el valor del bit U/L. Véase el esquema siguiente:

[55] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

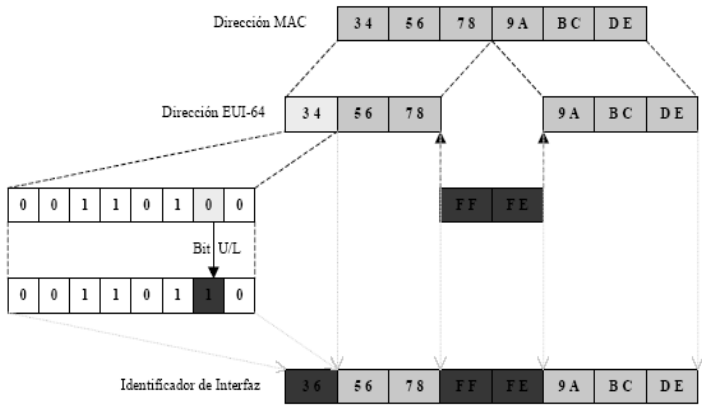


Figura 1.34: Grafica del Identificador EUI-64[56]

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

1.33.1.- MULTI-HOMING

El mecanismo de asignación de direcciones IPv6 es totalmente jerárquico. El multi-homing ("múltiples hogares") es el mecanismo por el cual un determinado sitio o red puede estar conectado a otros por múltiples caminos, por razones de seguridad, redundancia, ancho de banda, balanceo de carga, etc.

Dado que un determinado sitio utiliza el prefijo de su ISP, o proveedor de nivel superior, un sitio puede ser "multi-homed" simplemente teniendo varios prefijos. Frecuentemente, cada prefijo estará asociado a diferentes conexiones físicas, aunque no necesariamente, dado que se puede tratar de una sola conexión física y

[56] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

diversos túneles o conexiones virtuales. La problemática se plantea por la dificultad de que un host decida, en una red “multi-homed”, que dirección fuente utilizar.

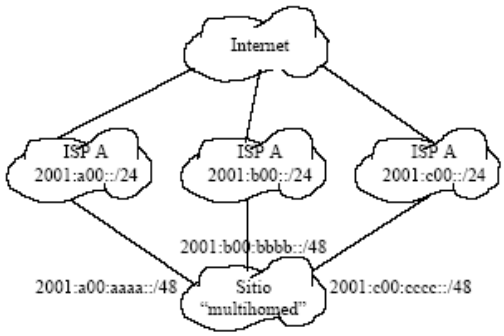


Figura 1.35: Funcionamiento del multi-homed[57]

Algunos de los documentos sobre los que se está trabajando en este campo son:

- Default Address Selections for IPv6
- IPv6 Multi-homing with Route Aggregation.
- Multi-homed Routing Domain Issues for IPv6.

1.33.2.- IPSEC

Una de las grandes ventajas de IPv6 es, sin duda, la total integración de los mecanismos de seguridad, autenticación y confidencialidad (encriptación), dentro del núcleo del protocolo. Se trata por tanto de algo obligatorio, y no adicional ni “añadido” como en IPv4. Para ello, la siguiente cabecera puede tener valores AH (autenticación – “Authentication Header”) y ESP (encriptación – “Encapsulation Security Payload”), que permiten, básicamente, emplear las mismas extensiones de protocolo empleadas en IPv4, y que de hecho, al haber sido desarrolladas con posterioridad al inicio de los trabajos de IPv6, ya lo contemplan. Dado que los

[57] http://www.ipv6.unam.mx/documentos/Taller-IPv6.pdf

mecanismos asociados ya han sido descritos, simplemente citamos las normas básicas que son aplicables: RFC2401 al RFC2412 y RFC2451.

1.34.- MOVILIDAD

La posibilidad de que un nodo mantenga la misma dirección IP, a pesar de su movilidad, es otra de las motivaciones básicas de IPv6. Como no, ya se han iniciado trabajos al respecto en IPv4, pero las complicaciones para usar la movilidad en este caso son enormes.

La idea básica permite identificar a un nodo móvil por su dirección de partida ("home address"), independientemente de su punto de conexión a Internet en cada momento dado. Por supuesto, cuando no esta en su punto de origen o de partida, también esta asociado con la información que permite identificar su posición o dirección actual ("care-of-address"). Los paquetes enviados a un nodo móvil (a su dirección de origen), son transparentemente encaminados a su "dirección actual".

El protocolo también permite que los nodos IPv6 almacenen la información de vinculación entre la dirección de partida y la posición actual, a modo de caché, y por tanto sean capaces de enviar los paquetes destinados al nodo móvil, directamente a su "dirección actual".
Para ello, el protocolo define nuevas opciones de destino, una de las cuales ha de ser soportada incluso en paquetes recibidos por todos los nodos (aunque no sean móviles).

Además, hay que prever, dada la estructura habitual de las redes inalámbricas (ejemplo muy habitual, la telefonía celular), que un nodo móvil puede estar conectado simultáneamente a varias redes (varías células que se solapan), y debe de ser alcanzable por cualquiera de ellas.

Los trabajos iniciales están documentados en el RFC2002 (soporte de movilidad en IP).

1.35.- DNS

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

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

Las extensiones han sido diseñadas para ser compatibles con las aplicaciones existentes y, en particular, con las implementaciones del propio DNS. El problema del sistema de DNS existente es fácilmente comprensible: Al hacer una consulta, las aplicaciones asumen que se les devolverá una dirección de 32 bits (IPv4). Para resolverlo, hay que definir las siguientes extensiones, antes indicadas:

- Un nuevo tipo de registro de recurso para mapear un nombre de dominio con una dirección IPv6: Es el registro AAAA (con un valor de tipo 28, decimal).
- Un nuevo dominio para soportar búsquedas basadas en direcciones. Este dominio es IP6.INT. Su representación se realiza en orden inverso de la dirección, separando los nibbles (hexadecimal) por puntos (“.”), seguidos de “.IP6.INT”. Así, la búsqueda inversa de la dirección 4321:0:1:2:3:4:567:89ab, seria

  “b.a.9.8.7.6.5.0.4.0.0.0.3.0.0.0.2.0.0.0.1.0.0.0.0.0.0.0.1.2.3.4.IP6.INT”

- Redefinición de las consultas existentes, que localizan direcciones IPv4, para que puedan también procesar direcciones IPv6. Ello incluye TODAS las consultas, lógicamente (NS, MX, MB, ...).

Además, para soportar la agregación de direcciones IPv6, la renumeración y el multi-homing, se trabaja en un nuevo tipo de registro de recurso (A6) para almacenar las direcciones IPv6 de forma que se agilice la renumeración de la red.

1.36.- PROTOCOLO DE ROUTING

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

1.36.1.- RIPng

La especificación del Protocolo de Información de Rutas (RIP – “Routing Information Protocol”) para IPv6, recoge los cambios mínimos e indispensables para su adecuado funcionamiento.

RIPng es un protocolo pensado para pequeñas redes, y por tanto se incluye en el grupo de protocolos de pasarela interior (IGP – “Interior Gateway Protocol”), y emplea un algoritmo denominado “Vector-Distancia”. Se basa en el intercambio de información entre routers, de forma que puedan calcular las rutas más adecuadas, de forma automática. RIPng sólo puede ser implementado en routers, donde requerirá como información fundamental, la métrica o número de saltos (entre 1 y 15), que un paquete ha de emplear, para llegar a determinado destino. Cada salto supone un cambio de red, por lo general atravesando un nuevo router. Además de la métrica, cada red tendrá un prefijo de dirección destino y la longitud del propio prefijo.

Estos parámetros han de ser configurados por el administrador de la red. El router incorporará, en la tabla de encaminado, una entrada para cada destino accesible (alcanzable) por el sistema. Cada entrada tendrá como mínimo, los siguiente parámetros:

- El prefijo IPv6 del destino.
- La métrica (número de saltos entre este router y el destino).
- La dirección IPv6 del siguiente router, así como la ruta para llegar a él.
- Un indicador relativo al cambio de ruta.
- Varios contadores asociados con la ruta.

Además se podrán crear rutas internas (saltos entre interfaces del propio router), o rutas estáticas (definidas manualmente). RIPng es un protocolo basado en UDP. Cada router tiene un proceso que envía y recibe datagramas en el puerto 521 (puerto RIPng).

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

1.36.2.- OSPFV6

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

Se trata de un protocolo de encaminado dinámico, que detecta rápidamente cambios de la topología (como un fallo en un router o interfaz) y calcula la siguiente

ruta disponible (sin bucles), después de un corto período de convergencia con muy poco tráfico de routing.

Cada router mantiene una base de datos que describe la topología del sistema autónomo (de la red), y es lo que denominamos base de datos de “estado de enlaces”. Todos los routers del sistema tienen una base de datos idéntica, indicando el estado de cada interfaz, y de cada “vecino alcanzable” .Los routers distribuyen sus “estados locales” a través del sistema autónomo (la red) por medio de desbordamientos (“flooding”). Todos los routers utilizan el mismo algoritmo, en paralelo, y construyen un árbol de las rutas más cortas, como si fueran la raíz del sistema. Este árbol de “rutas más cortas” proporciona la ruta a cada destino del sistema autónomo.

Si hubiera varias rutas de igual coste a un determinado destino, el tráfico es distribuido equilibradamente entre todas. El coste de una ruta se describe por una métrica simple, sin dimensión. Se pueden crear áreas o agrupaciones de redes, cuya topología no es retransmitida al resto del sistema, evitando tráfico de routing innecesario. OSPF permite el uso de máscaras diferentes para la misma red (“variable length subnetting”), lo que permite el encaminado a las mejores rutas (las más largas o más específicas).

Todos los intercambios de protocolo OSPF son autenticados, y por tanto sólo pueden participar los routers verificados (“trusted”). OSPFv6 mantiene los mecanismos fundamentales de la versión para IPv4, pero se han tenido que modificar ciertos parámetros de la semántica del protocolo, así como el incremento del tamaño de la dirección. OSPFv6 se ejecuta basado en cada enlace, en lugar de en cada subred. Además, ha sido necesario eliminar la autenticación del protocolo OSPFv6, dado que IPv6 incorpora estas características (AH y ESP).

A pesar de la mayor longitud de las direcciones, se ha logrado que los paquetes OSPFv6 sean tan compactos como los correspondientes para IPv4, eliminando incluso algunas limitaciones y flexibilizando la manipulación de opciones.

1.36.3.- BGP4+

El Protocolo de Pasarelas de Frontera (BGP – “Border Gateway Protocol”) es un protocolo de encaminado para la interconexión de sistemas autónomos, es decir, para el enrutado entre diferentes dominios.

Frecuentemente se emplea para grandes corporaciones y para la conexión entres proveedores de servicios (como ISP’s). Su principal función es, por tanto, el intercambio de información de disponibilidad o alcance entre varios sistemas BGP, incluyendo información de los sistemas autónomos que contienen, permitiendo así construir las rutas más adecuadas y evitar bucles de tráfico.

BGP4 incorpora mecanismos para soportar enrutado entre dominios sin clases (“classless interdomain routing”), es decir, el uso de prefijos, agregación de rutas, y todos los mecanismos en los que se basa IPv6. BGP se basa en que un dispositivo sólo informa a los otros dispositivos que se conectan a él, acerca de las rutas que el mismo emplea. Es decir, es una estrategia de “salto a salto”. La implicación es la simplicidad de Internet, pero la desventaja es que este mecanismo impide políticas complejas, que precisan de técnicas como el enrutado de fuente (“source routing”).

BGP usa TCP como protocolo de transporte, a través del puerto 179. BGP4+ añade a BGP (RFC1771), extensiones multiprotocolo, tanto para IPv6 como para otros protocolos, como por ejemplo IPX.

CAPITULO II

DESARROLLO DE LA METODOLOGIA DE REDES IPV4 A IPV6

En la actualidad se está introduciendo gradualmente el IPv6. Sin embargo, resulta necesario acelerar este proceso para evitar que las actuales desventajas del IPv4 obstaculicen el desarrollo de Internet y el uso de las nuevas tecnologías.

A continuación presentamos algunas de las estrategias de implantación que nos permitirá acceder a las ventajas que nos brinda el nuevo protocolo.

2.1.- MIGRACION Y COEXISTENCIA

Actualmente existen varios métodos que nos permiten realizar una fácil implementación del nuevo protocolo IPv6; estos métodos fueron diseñados para facilitar una convivencia transitoria entre IPv6 e Ipv4, hasta que toda red trabaje con este nuevo protocolo. Los métodos creados surgen como una solución a varios problemas que al momento tenemos que afrontar al trabajar con IPv6, entre los principales problemas tenemos.

- IPv4 e Ipv6 es Incompatible a nivel de paquete: es decir que actualmente los nodos finales actuales de Internet no generan, ni reconocen paquetes IPv6, además los routers IP actuales descartan paquetes Ipv6.

- Dificultad para migrar toda la red de Internet ya que no se puede migrar a Ipv6 en forma inmediata, por lo que en una etapa intermedia se deberá trabajar con Ipv4 e Ipv6 a nivel lógico.

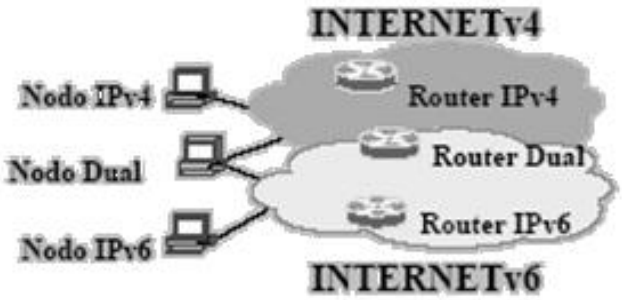


Figura 2.1: Compatibilidad de nodos IPv4 e Ipv6 en Internet[58]

Por estos motivos se han implementado métodos que permitan la integración y/o interacción de sistemas Ipv4 e IPv6 que a continuación se describe.

Según el punto donde nos encontremos y para conseguir la comunicación, podemos hablar de los siguientes métodos:

1. Mecanismo de tipo Tunel (En la red: tunelización)
2. Mecanismos de Traducción (En el gateway: traductores IPv4/IPv6)

1.- Mecanismos de Tipo Túnel: Es un mecanismo para comunicación entre islas IPv6; estos túneles se basan en la encapsulación de paquetes IPv6 dentro de paquetes Ipv4.

Los túneles proporcionan un mecanismo para utilizar las infraestructuras IPv4 mientras la red IPv6 esta siendo implantada. Este mecanismo consiste en enviar datagramas IPv6 encapsulados en paquetes IPv4. Los extremos finales del túnel

[58] http://www.techsupportalert.com/

siempre son los responsables de realizar la operación de encapsulado del paquete/es IPv6 en IPv4.

Los túneles se clasifican según el mecanismo por el cual realizan el encapsulado del nodo extremo del túnel. En los casos (router a router y host a router), el paquete IPv6 es tunelizado a un router. El extremo final de este tipo de túnel, es un router intermedio que debe desencapsular el paquete IPv6 y reenviarlo a su destino final. En este caso, el extremo final del túnel es distinto del destino final del paquete, por lo que la dirección en el paquete IPv6 no proporciona la dirección IPv4 del extremo final del túnel. La dirección del extremo final del túnel ha de ser determinada a través de información de configuración en el nodo que realiza el túnel. Es lo que se denomina "túnel configurado", describiendo aquel tipo de túnel donde el extremo final del túnel es explícitamente configurado.

En los otros dos casos (host a host y router a host), el paquete IPv6 es tunelizado, durante todo el recorrido, a su nodo destino. El extremo final del túnel es el nodo destino del paquete, y por tanto, la dirección IPv4 está contenida en la dirección IPv6. Este caso se denomina "túnel automático".

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

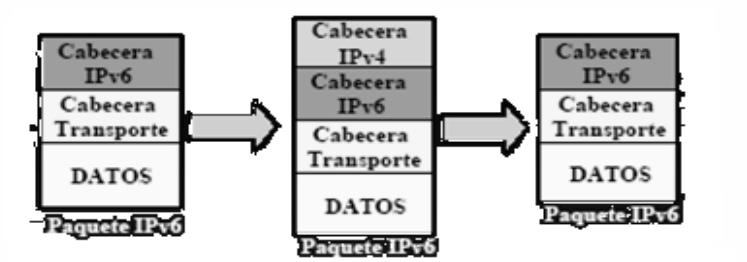


Figura 2.2: Método para encapsular paquetes IPv6[59]

[59] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

Entre los mecanismos de tunelización tenemos:

- Túneles Manuales
- Túneles Automáticos
- Túneles 6to4
- 6over4
- ISATAP (Intra-site automatic Túnel Addessing Protocol)

2.- Mecanismos de Traducción: Son mecanismos para la comunicación de nodo IPv6; Una vez unidas varias islas IPv6 el problema que se plantea es el de que todos los nodos puedan acceder a la Internet Ipv6 como a la Ipv4. La solución va a consistir nivel de aplicación, transformando la capa de enlace o asignando temporalmente direcciones IPv4 a nodos IPv6. Existen varios mecanismos que nos permiten realizarlo, y a continuación tenemos:

.

- Doble Pila o Dual Stack
- SIIT (Stateless IP-ICMP translation algorithm)
- NAT-PT (Network address translation - protocol translation)
- BIS (Bump in the stack)
- SOCK64
- SOCKv5

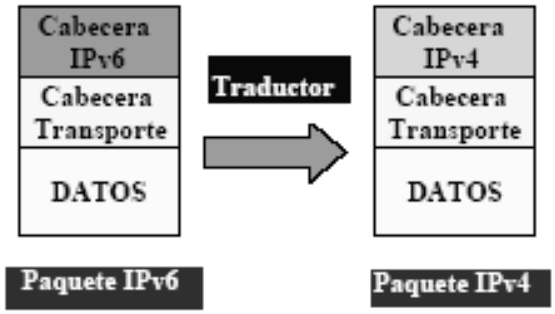


Figura 2.3: Mecanismos de traducción de paquetes IPv6 a IPv4[60]

2.1.1.- Túneles Manuales

Este mecanismo se encarga de interconectar islas IPv6 a través de un océano IPv4.Cada extremo es un nodo dual y en ellos se configura las direcciones IPv4 e IPv6 tanto local como remotas.

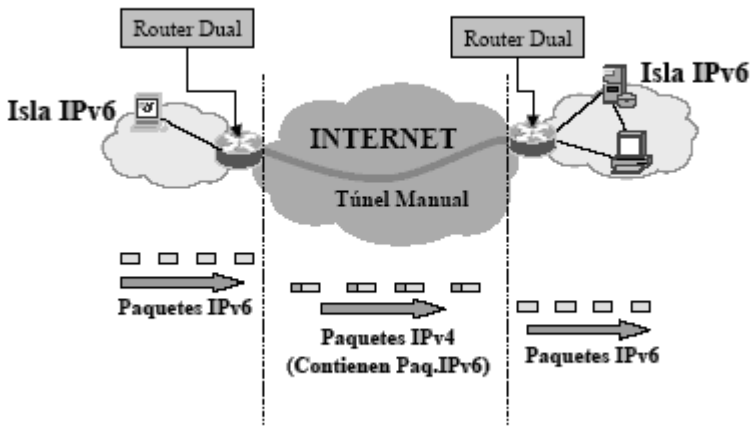


Figura 2.4: Interconexión de túneles manuales[61]

[60] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

[61] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

Entre las ventajas que tenemos en este mecanismo son las siguientes:

- Es un método muy utilizado en el acceso al 6-Bone[62].
- Se encuentra disponible en múltiples plataformas (Cisco, Linux, Solaris, Windows NT)[63].
- Es un método totalmente transparente respecto al nivel IPv6 y superiores, con lo cual no afecta a las aplicaciones.
- No consume excesivos recursos, la MTU[64] se reduce en 20 bytes (cab. IPv4 típica).
- Aplicación Principal: Conexión con ISP[65] IPv6 remoto a través de Internet.

Estos mecanismos se hacen indispensables para labores de investigación, dado que se requieren direcciones IPv6 y nombres DNS permanentes. el "Tunnel Broker" no requiere la configuración de un router. Se trata de ISP's IPv6 "virtuales", proporcionando conectividad IPv6 a usuarios que ya tienen conectividad IPv4.

El "tunnel broker" es el lugar donde el usuario se conecta para registrar y activar "su túnel". El "broker" gestiona (crea, modifica, activa y desactiva) el túnel en nombre del usuario.

El "tunnel server" es un router con pila doble (IPv4 e IPv6), conectado a Internet, que siguiendo órdenes del "broker" crea, modifica o borra los servicios asociados a un determinado túnel/usuario. El mecanismo para su configuración es sencillo. El servidor de túneles crea los registros DNS, el extremo final del túnel, y genera un script para la configuración del cliente.

Características

[62] Proyecto IPv6 creado en México y unido a la mayor parte de los países del mundo con propósito de utilizar el protocolo Ipv6
[63] Sistemas Operativos de uso Cliente / Servidor
[64] Máxima unidad de transferencia
[65] Proveedor de servicios de Internet

- Sistema de Alta de Túneles con interfaz WEB.
- ISP v6 proporcionan acceso al 6-Bone y son accesibles por Internet.
- Opcionalmente: Detecta tiempos de inactividad y liberar recursos.
- Posee implementaciones en Windows NT, Linux.

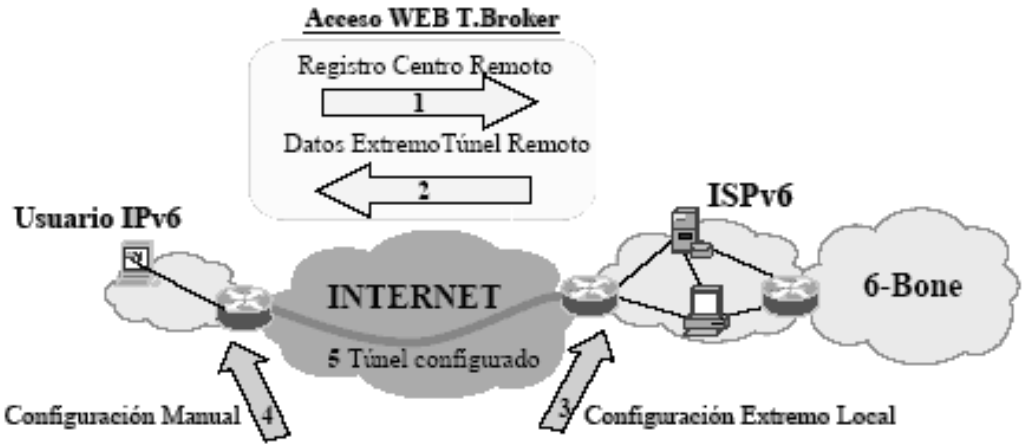


Figura 2.5: Tunnel-Broker y Tunnel Server[66]

2.1.2.- Túneles Automáticos

Permite a nodos duales comunicarse a través de una infraestructura IPv4; Las direcciones IPv6 son compatibles con las direcciones IPv4 ya que el prefijo de IPv6 se aumenta a la dirección IPv4.

[66] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

Prefijo 0::/96 + Dirección IPv4
Dirección IPv4 aumentada el prefijo IPv6 para poder establecer comunicación

Tabla 2.1: Direccionamiento a través de túneles automáticos

Se define una interfaz virtual para la dirección “IPv4 Compatible”; y los paquetes destinados a direcciones “IPv4 Compatible” se envían por el túnel automático surgiendo las siguientes reglas:

- Dirección origen IPv6: Es una dirección local y es enviada a través de direcciones IPv4 Compatible.
- Dirección Destino IPv4: Esta es dirección remota y se obtiene de la dirección “IPv4 Compatible” .

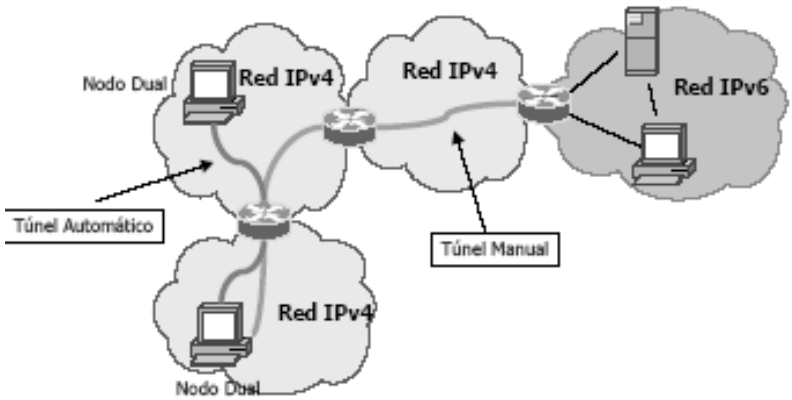


Figura 2.6: Uso Túneles Automáticos y Túneles Manuales [67]

[67] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

2.1.3.- Túneles 6to4 (Túneles IPv6 entre Ipv4)

Se utiliza para conectar dominios IPv6 aislados en un entorno IPv4; Es una especie de tunelización automática que no precisa direcciones compatibles con IPv4; Los puntos IPv4 finales del túnel se identifican en el prefijo del dominio IPv6

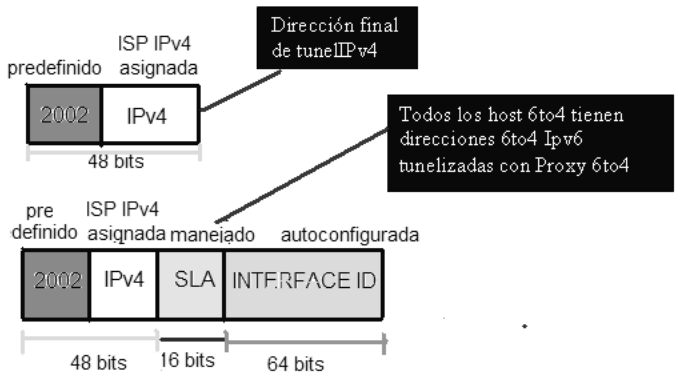


Figura 2.7 : Prefijo 6to4 y dirección 6to4[68]

- Router 6to4
  - √ Router que se encuentra entre un área amplia que trabaja en IPv4 y un sitio IPv6
  - √ La encapsulación y la desencapsulación se lleva a cabo en el router 6to4

- Host 6to4
  - √ Host el cual tiene una dirección 6to4

[68] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

- Router de paso
  - √ Router 6to4 que soporta el encaminamiento de tránsito entre una dirección 6to4 y una dirección IPv6 nativa
  - √ El router de paso tiene al menos un pseudo interfaz 6to4 lógico y al menos un interfaz IPv6
  - √ Anuncia el prefijo 6to4 y el prefijo IPv6 nativo

Este mecanismo funciona aún cuando la dirección IPv4 global (pública) es única y se accede a la red mediante mecanismos NAT (Network Address Translation), que es el caso más común en las redes actuales para el acceso a Internet a través de ISP's.

A cada isla IPv6 se le asigna un prefijo :

2002::/16 + Dir.IP Router
Dirección IPv6 asignada un prefijo de Dirección de router IPv4

Tabla 2.2: Direcciones tunelizadas a través de 6to4

El siguiente salto es a un host con IPv4 conteniendo la dirección IPv6, y el encaminamiento entre las distintas islas se apoya en el encaminamiento IPv4 ya asignado.

Actualmente se encuentra implementaciones en Windows NT y en el Proyecto KAME[69]: bajo Linux y FreeBSD.

[69] Proyecto creado bajo plataforma FreeBSD para conexión IPv6

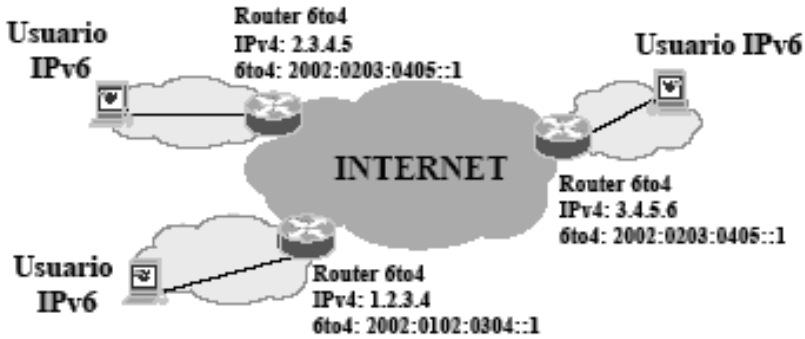


Figura 2.8: Funcionamiento del túnel 6to4[70]

Entre las ventajas tenemos que al igual que los túneles manuales, son transparentes a nivel IPv6 y, por tanto, no afectan a las aplicaciones.

- Se trata de túneles establecidos dinámicamente y sin configuración previa.
- Dadas N islas IPv6, sólo se establecen los túneles necesarios para las conexiones activas en cada momento.

2.1.4.- Túneles 6over4 (Túneles IPv6 sobre IPv4)

También denominado transmisión de IPv6 sobre dominios IPv4. Este mecanismo permite a hosts IPv6 aislados, sin conexión directa a routers IPv6, ser totalmente funcionales como dispositivos IPv6.

Para ello se emplean dominios IPv4 que soportan multicast como su enlace local virtual. Es decir, usamos multicast IPv4 como su “ethernet virtual”.

[70] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

De esta forma, estos hosts IPv6 no requieren direcciones IPv4 compatibles, ni túneles configurados.

Los extremos finales del túnel se determinan mediante Neighbor Discovery. Es decir que para los procesos se necesita de Neighbor/Router Discovery; Es imprescindible que la subred IPv4 soporte multicast.

Mediante este mecanismo se puede decir que los nodos IPv6 dispersos en subredes IPv4 forma una "LAN virtual" IPv6 dándose el tráfico IPv6 entre nodos encapsulado en IPv4 empleando direcciones IPv4 Multicast.

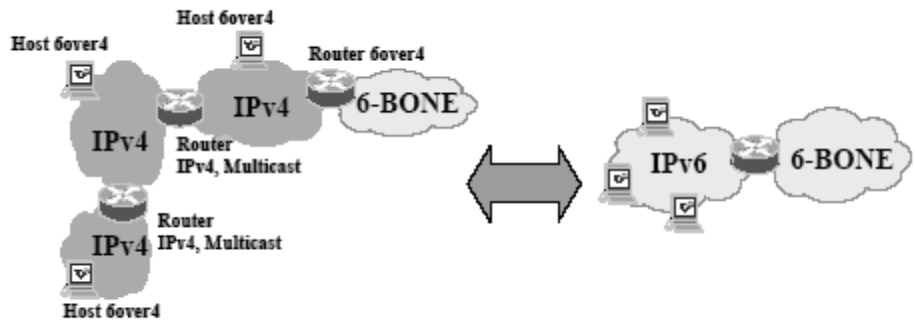


Figura 2.9: Router 6over4 con acceso 6-BONE[71]

- Al igual que los túneles anteriores, son transparentes a nivel IPv6 y, por tanto, no
  afectan a las aplicaciones.
- Se trata de túneles establecidos dinámicamente y sin configuración previa.
- Permite probar IPv6 en algunos nodos de una red IPv4 corporativa sin instalar el stack IPv6 en los routers internos.

[71] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

- Instalando en un solo router el stack IPv6 y conectándolo al 6-Bone se proporciona acceso a dicha red a todos al resto de nodos IPv6.

2.1.5.- (Intra-site automatic Túnel Addessing Protocol) ISATAP

Como su nombre lo indica, este método también está pensado para la comunicación de nodos de un mismo sitio, tiene algunas ventajas respecto a 6over4, como que no necesita multicast IPv4 y que soluciona los problemas que se da cuando una misma organización no tiene toda a misma red en un solo lugar.

La técnica funciona empotrando la dirección IPv4 del nodo en el identificador del interfaz. Puesto que este método viene a solucionar los problemas de comunicación dentro de un sitio, las direcciones IPv4 no tiene por que ser globales.

Esto significa que aunque exista NAT[72], el mecanismo seguirá funcionando correctamente.

2.1.6.- Doble Pila o Dual Stack

Este mecanismo provee de soporte completo para ambos protocolos IPv4 e IPv6 en Hosts y Routers.

1. Devuelve sólo direcciones IPv6
2. Devuelve sólo direcciones IPv4
3. Devuelve direcciones de ambas versiones del protocolo (IPv4 e IPv6)

[72] **T**raducción de **D**irecciones de **R**edes.- NAT hace referencia al proceso de conversión de las direcciones IP utilizadas en una red privada a direcciones IP de Internet.

El camino más lógico y evidente de transición es el uso simultáneo de ambos protocolos, en pilas separadas. Los dispositivos con ambos protocolos también se denominan “nodos IPv6/IPv4”.

De esta forma, un dispositivo con ambas pilas pueden recibir y enviar tráfico a nodos que sólo soportan uno de los dos protocolos (nodos sólo IPv4 o sólo IPv6). El dispositivo tendrá una dirección en cada pila. Se pueden utilizar direcciones IPv4 e IPv6 relacionadas o no, y se pueden utilizar mecanismos manuales o automáticos para la asignación de las direcciones.

El DNS podrá devolver la dirección IPv4, la dirección IPv6, o ambas.

Se pueden emplear la dirección IPv4 (32 bits), anteponiéndole 80 bits con valor cero y 16 bits con valor 1, para crear una dirección IPv6 “mapeada desde IPv4”.

Los túneles pueden ser utilizados de formas diferentes unidos a la técnica de doble pila:

1. Router a router. Routers con doble pila (IPv6/IPv4) se conectan mediante una infraestructura IPv4 y transmiten tráfico IPv6. El túnel comprende un segmento que incluye la ruta completa, extremo a extremo, que siguen los paquetes IPv6.
2. Host a router. Hosts con doble pila se conectan a un router intermedio (también con doble pila), alcanzable mediante una infraestructura IPv4. El túnel comprende el primer segmento de la ruta seguida por los paquetes.
3. Host a host. Hosts con doble pila interconectados por una infraestructura IPv4. El túnel comprende la ruta completa que siguen los paquetes.
4. Router a host. Routers con doble pila que se conectan a hosts también con doble pila. El túnel comprende el último segmento de la ruta.

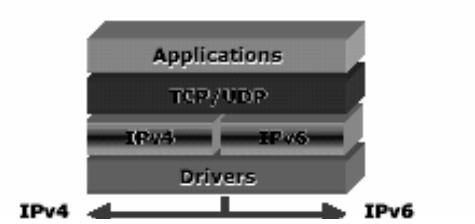


Figura 2.10 : Resolución de operaciones con IPv4/IPv6Dual Stack[73]

2.1.7 .- SIIT (Stateless IP- ICMP translation algorithm)

Es un mecanismo que especifica la traducción de encabezados IP/ICMP entre IPv6 e IPv4. Como no tiene en cuenta el estado del paquete (stateless), hace la traducción para todos los paquetes. Esta traducción queda limitada a la cabecera IP; No se realiza un control de estado, por lo que la traducción se debe realizar por cada paquete.

2.1.8 .- NAT-PT (Network address translation - protocol translation)

El NAT Tradicional.- Traduce direcciones (conexión de redes con dir. IPv4 privado).
NAT-PT.- Traducción de direcciones y protocolo, esta traducción están basada en el mecanismo de traducción SIIT (Stateless IP- ICMP translation algorithm).

No es transparente a nivel de aplicación; Precisa algunas extensiones:

- DNS-ALG: Transforma peticiones DNS IPV4 “WWW” a peticiones de DNS IPv6 “AAAA[74]”

[73] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

[74] AAAA.- DNS para IPv6

- FTP-ALG: Las conexiones con FTP son problemáticas pues abren dos conexiones TCP intercambiando direcciones IP a nivel de aplicación.

Se utiliza para comunicaciones entre hosts que son sólo IPv6 e IPv4 respectivamente En realidad es NAT (se usa el mecanismo NAT para la asignación de la dirección IPv4) + el Protocolo de Traducción (se usa el mecanismo SIIT). Se realiza la traducción IPv4/IPv6 y se mantiene el estado mientras dura la sesión.

Traducción de direcciones o Utiliza el fondo de direcciones de IPv4, y mantiene la tabla de mapeado de la dirección IPv4/IPv6; Protocolo de traducción IPv4 ⟷ IPv6

Se usa SIIT (Stateless IP/ICMP Translation); Provee de una regla de traducción de cabeceras entre IPv4 IPv6.⟷

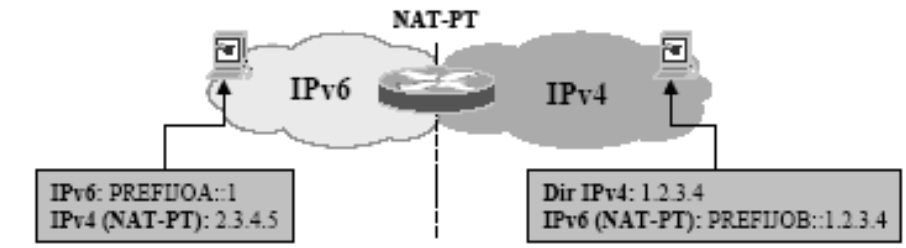


Figura 2.11: Conexión de IPv6 a IPv4 por NAT-PT[75]

NAT-PT tiene ventajas como:

[75] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

- Muchas redes corporativas poseen experiencia en la gestión/administración de NATs.
- Implementado en la mayor parte de los routers (Cisco, Telebit, Linux) y en algunas plataformas habituales en nodos finales (Windows 2000).
- Si la comunicación extremo-a-extremo es heterogénea (IPvX-IPvY) NAT-PT resulta adecuado (teniendo en cuenta siempre la carga de tráfico prevista).

2.1.9 .- BIS (Bump in the stack)

Es un caso particular del NAT-PT. A un nodo Ipv4 se le agregan tres módulos a su pila para cuando necesite comunicarse con nodos Ipv6, estos son unas extensiones al resolvedor de nombres, un mapeador de direcciones y un traductor. La idea es que cuando un máquina Ipv4 necesite comunicarse con un nodo Ipv6, a su dirección Ipv6 se le asigna una dirección Ipv4 de un rango de direcciones que tiene la maquina. La traducción completa del paquete se hace de acuerdo a SIIT.

2.1.10 .- SOCK64

SOCKS es una Puerta de Enlace (Gateway) entre dos redes que permite que ciertas aplicaciones se comuniquen con sus contrapartes en la otra red, en este caso desde una red Ipv4 a una Ipv6 o viceversa.

La comunicación a través de un servidor SOCKS es dependiente de la aplicación, esto quiere decir que si alguna aplicación no tiene soporte para SOCKS no se va a poder comunicar con su contraparte. Además es un solo punto de falla.

2.1.11.- SOCKv5

Uso tradicional SOCKSv5: conectividad IP directa a Internet en redes con firewall a determinados hosts.

- √ Servidor SOCKSv5 dual Traductor de Protocolos (Algoritmo SIIT).
- √ Traducción IPv4-IPv6 y viceversa. Conexiones SIEMPRE iniciadas por cliente.
- √ Dos componentes: Servidor SOCKSv5 + Librería SOCKSv5 (cliente).

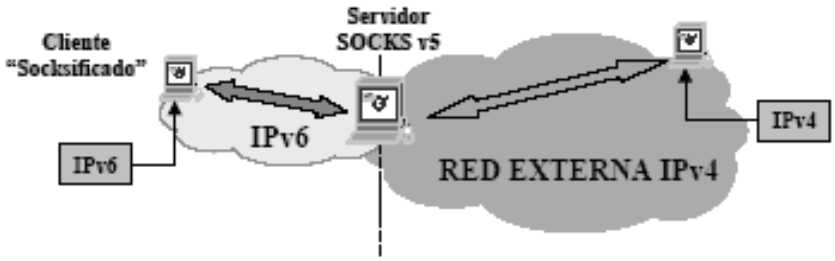


Figura 2.12: Conexión a través de SOCKv5[76]

Procedimiento del mecanismo SOCKSv5 de la figura 2.14

1. Una aplicación en el nodo cliente sobre IPv4 inicia una conexión TCP o UDP con un nodo externo empleando el nombre completo
2. La librería SOCKSv5 en el cliente intercepta la resolución del nombre ("gethostbyname") e inicia una conexión TCP al puerto 1080 del servidor SOCKSv5.
3. El servidor SOCKSv5 devuelve al cliente SOCKSv5 una dirección IPv4 remota falsa ("fake IPv4 address").
4. El servidor SOCKSv5 inicia la conexión TCP o UDP con el nodo remoto IPv6 y hace de proxy entre el cliente y el nodo externo. Si el nodo externo es IPv6, aplica además el algoritmo de traducción SIIT.

[76] http://playground.sun.com/pub/ipng/html/ipngimplementations.html

5. En el cliente, los paquetes con la “fake IPv4 address” como origen o destino son interceptados y tratados por la librerías SOCKSv5 que los recibe o envía respectivamente al servidor SOCKSv5.

2.2 SITUACION ACTUAL DE IPv6

Dentro del Proyecto “UNAM IPV6[77]” en México se estableció un amplio programa de pruebas y trabajos con temas como: implementaciones, stacks IPv4/IPv6, túneles, software de conexión, aplicaciones multimedia, servidores para Web y DNS, autoconfiguración, calidad de servicio, IPv6 sobre ATM, conexión con redes internacionales de IPv6 (6Bone, 6REN), etc.

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

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

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

[77] Nodo IPv6 : Proyecto creado para la interconexión de redes IPv6 para toda América.

Actualmente se esta trabajando con instituciones mexicanas y de América Latina para realizar su conexión IPv6 hacia la UNAM.

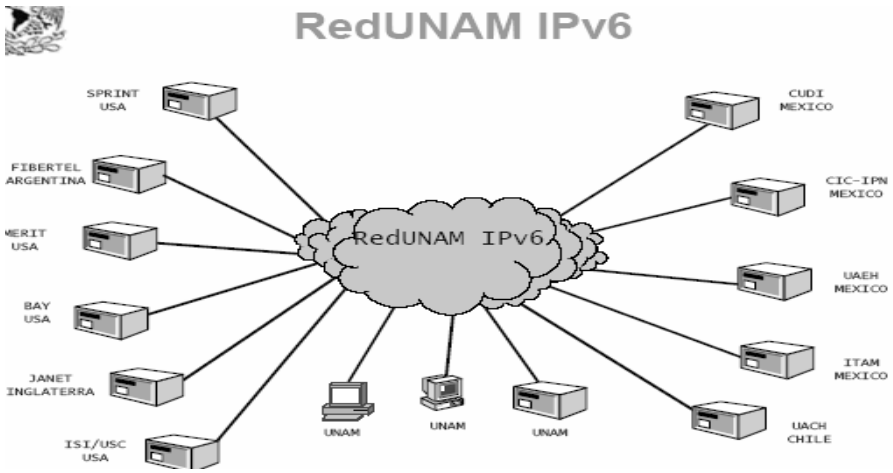
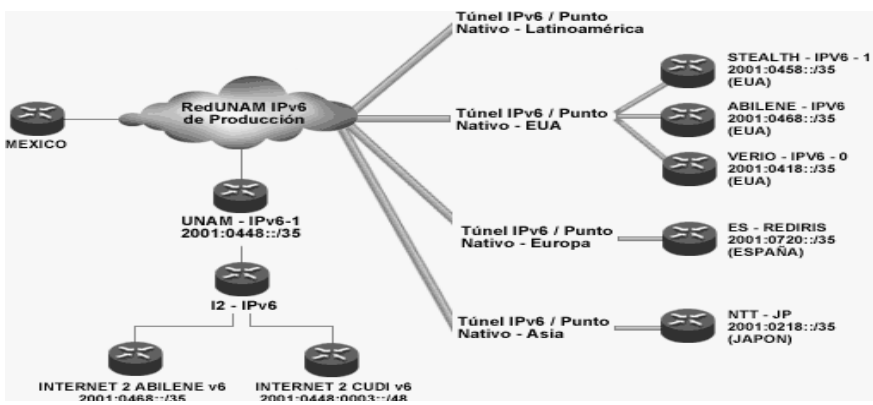


Figura 2.13: Red UNAM IPv6 para pruebas[78]

- Disponible para pruebas nacionales e internacionales.
- Se pueden configurar túneles y delegar espacio de direcciones IPv6.



[78] http://ww

Figura 2.14: Red UNAM IPv6 para producción[79]

- Servicios de Internet basados en IPv6.
- Para usuarios en México y Latinoamérica

En lo que se refiere al estado de desarrollo de IPv6 se ha identificado en cinco regiones:

Norteamérica: Actualmente las redes que se encuentran en Norteamérica pueden ser localizadas en torno al "6Bone", la plataforma de pruebas internacional de IPv6 (http://6bone.net/). Otras actividades relacionadas con IPv6 que incluyen importantes participaciones norteamericanas son 6REN (http://www.6rem.net/), redes de investigación y educación, 6TAP (http://www.6tap.net/), iniciativa para proporcionar un router Ipv6 central en Chicago para facilitar la interconexión entre redes IPV6, (http://www.freenet6.net/) y (http://www.viagenie.qc.ca/), iniciativa de túneles automáticos.

Asia: En esta área, el impacto de la falta de direcciones IPv4 ha sido más obvio, y APNIC, la entidad de registro regional de Internet para esta zona (http://www.apnic.net/) espera agotar su rango de direcciones IPv4 en muy pocos meses.

[79] http://www.unam.net.mx

Europa: La industria de la telefonía móvil es un soporte muy fuerte para la transición a IPv6. En correspondencia, ETSI (European Telecomunications Standards Institute) y el Foro IPv6 han establecido un acuerdo de cooperación para unir sus fuerzas.

Rusia: Las fuertes relaciones entre el Foro Ipv6, el Foro local Ruso, y el Frente (red académica y de investigación Rusa). El objetivo es crear una comunidad rusa de usuarios de IPv6 y proveedores de servicios y soluciones.

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

Ecuador : Actualmente dentro del Ecuador no se tiene ninguna implantación sobre IPv6; En cuanto a los ISP´s no ofrecen este servicio y lo ven como un proyecto a largo plazo; con respecto al Software es asequible pero en cuanto al Hardware no ya que no existe tecnología suficiente dentro del país que soporte este protocolo.

Países que se encuentran unidos a IPv6 – 6Bone

Figura 2.15: IPv6 en Latinoamérica[80]

En la actualidad se están realizando los siguientes proyectos, pruebas y eventos:

Proyectos

- Red nativa de IPv6 en Internet en Latinoamérica.
  En colaboración con el Grupo de Trabajo de IPv6 de AMPATH (Red de las Américas)
- Desarrollo y programación de aplicaciones con soporte IPv6.
  Soporte de Multicast con IPv6 en el Backbone.

- Uso de aplicaciones de videoconferencia con soporte IPv6.

Pruebas

- Aplicaciones de videoconferencia con soporte IPv6

[80] http://www.unam.net.mx

- Herramientas de seguridad.
- Pruebas con diferentes aplicaciones con soporte IPv6.

2.3 PROPUESTA METODOLÓGICA

Utilizar Ipv6 como protocolo para comunicación entre equipos de la Intranet de la ESPE-L será la mejor decisión, dadas las deficiencias claramente ya expuestas que posee IPv4, sin embargo, esta no es una decisión que se puede tomar sin el apoyo de los encargados del Departamento Informático de la Institución, ni tampoco sin un adecuado plan de trabajo que permita afrontar este cambio con los menores inconvenientes posibles.

La información detallada a continuación dará los lineamientos básicos para que la institución pueda migrar hacia este nuevo protocolo.

Las etapas a seguir para poder migrar de IPv4 a IPv6 serán:

I Etapa de Información y motivación
II Etapa de Definición de Objetivos y Visión
III Etapa de Estudio de la Organización (Intranet de la ESPE-L)
IV Etapa de Elaboración del Plan de Trabajo.
V Etapa de Pruebas, Instalación y Puesta en Funcionamiento.

I Etapa de Información y motivación

Esta etapa consiste básicamente en conocer las expectativas acerca del protocolo IPv6 tomando como universo al Departamento de Organización y Sistemas, Profesores de la Facultad de Sistemas y alumnos de los últimos niveles de la misma Facultad; dentro de los alumnos que se tomarán en cuenta son los que se encuentran en IV, V, VI, VII, VIII y IX nivel ya que estos cuentan con el conocimiento suficiente sobre las materias básicas sobre redes de acuerdo con la malla curricular; además se brindará información básica sobre IPv6, pero más que todo se motivará e instruirá sobre los beneficios que hacen importante a esta nueva tecnología.

Esta etapa se subdividirá en:

1.- Realización de cuestionarios: Estarán enfocados hacia el personal del Departamento de Sistemas, Profesores y estudiantes de los últimos niveles ya mencionados antes y nos permitir saber sus conocimientos y expectativas hacia este nuevo protocolo. En este paso se deberá tomar en cuenta aspectos como:

- Conocimientos básicos de IPv4 (Tipos de direcciones: A,B,C, Tamaños de la dirección, mascaras de subred, protocolos de enrutamiento.)
- Expectativas acerca de un posible cambio.
- Conocimientos acerca de IPv6.

2.- Realización de entrevistas: Estas irán enfocadas hacia la parte profesores, al igual que al personal del Departamento de Sistemas de Organización y Sistemas, se le preguntará sus conocimientos y expectativas, y al mismo tiempo serán informados a breves rasgos sobre el funcionamiento del nuevo protocolo y todos sus beneficios. Para esto se deberá hacer preguntas como:

- Problemas obtenidos con IPv4
- Conocimientos acerca de IPv6
- Expectativas del departamento técnico a cargo del posible cambio al protocolo IPv6, esto nos podrá hacer saber si la parte ejecutiva está al tanto de la posible migración.
- Expectativas con relación a uso del nuevo protocolo.

3.- Explicación básica: Estas irán enfocadas al personal de Departamento Organización y Sistemas, Profesores y alumnos encuestados y entrevistados y

tendrá como objetivo aumentar el nivel de conocimientos acerca de este nuevo protocolo. Se deberán indicar aspectos relacionados a:

- Desventajas de IPv4
- Ventajas de IPv6
- Formato del paquete de IPv6
- Tipo de direcciones Ipv6
- Direcciones mejoradas de IPv6
- Aplicaciones con soporte en IPv6
- Mecanismos de transición IPv6.

II Etapa de Definición de Objetivos y Visión

Una vez completamente informados sobre el tema se deberá definir una visión, o sea "Como será la Institución luego de las implementaciones de este protocolo" y seguidos de los objetivos. Estos objetivos deberán ser claros, concretos y estar dentro de los parámetros definidos.

III Etapa de Estudio de la Organización (Intranet de la ESPE-L)

Esta sin duda es la parte más compleja ya que tendremos que averiguar sobre aspectos físicos y lógicos de la Intranet de la ESPE-L

Entre estos aspectos tenemos que averiguar son:

- Número de máquinas dentro de la ESPE-L
- Sistemas Operativos que utilizan las máquinas.
- Tipo de red (Ethernet, Tocken Ring).
- Velocidad de la red (10MHz, 100MHz, 1GHz).
- Elementos (Switchs, Routers, HUB)

- Servicios de red (DNS, Mail, Servidores Web, Directorios, Bases de Datos).

Es de suma importancia prestar atención a los elementos de red y Sistemas operativos ya que fundamente la migración se basa en estos aspectos, por que la gran mayoría de ellos no soportan el nuevo protocolo y se deberá descargas de Internet paquetes parches que permita una normal operación.

IV Etapa de Elaboración del Plan de Trabajo.

Una vez recolectada la información necesaria, se deberá elaborar un plan que vaya de acuerdo a los objetivos y visión de la ESPE-L.

Entre los aspectos a tener en cuenta en la elaboración del plan de trabajo tenemos:

1. Selección de número de PC´s a ocupar IPv6.
2. Seleccionar el número de PC´s que ocuparan IPv4
3. Descripción de los dispositivos y aspectos para la conexión
4. Elección del software que soporte al nuevo protocolo.
5. Análisis y características del Software a emplear para en los computadores (clientes, Servidores y Enrutadores).
6. Elección del tipo de Direcciones de Red a ocupar (locales, de sitio, globales).
7. Elección de mecanismos de comunicación entre las máquinas que van a utilizar IPv4/IPv6.

V Etapa de Pruebas, Instalación y Puesta en Funcionamiento.

En esta etapa se tomará en cuenta los requisitos que se obtuvieron en la cuarta etapa ya que es necesario para poner en marcha la migración; esta etapa también contiene conjunto de pasos a seguir que son:

1. Configuración del protocolo ipv6 en diferentes sistemas operativos
   1.1 implementación del protocolo ipv6 sobre Microsoft Windows XP
   1.2 implementación del protocolo ipv6 sobre Windows 2000 Server
   1.3 implementación del protocolo ipv6 sobre Windows 2003 Server
   1.5 implementación del protocolo ipv6 sobre Linux

2. Implementación de tunneling
   2.1. Configuración de tunneling manual
   2.2. Configuración de tunneling autoconfigurado

3. Configuración de domain name system “DNS” mediante el protocolo IPv6
4.- Pruebas de conectividad con el protocolo ipv6 entre cliente servidor
5.- Configuración de nuevas direcciones de red Globales y locales y de sitio
6.- Comprobación de las ventajas del protocolo IPv6 (Neigbort Discovery)
7.- Asignación de dirección y creación de cliente Pv6 mediante Internet al 6bone

CAPITULO III

3.- APLICACIÓN DE LA METODOLOGIA EN LA RED DE LA ESPE-L

3.1 IMPLANTACION DE METODOLOGÍA

La parte más importante dentro del proyecto de la migración es el desarrollo de la metodología, ya que esta servirá de guía para que en un futuro se aplique dentro de las redes de la ESPE-L cuando llegue el momento determinado.

La metodología de Migración de Redes IPv4 a redes IPv6 consiste en cinco etapas las cuales nos entregan un estudio completo sobre la estructura de red de la ESPE-L y como manejarla al momento de la migración, las cuales cada una de ellas nos informan paso a paso sobre necesidades e inquietudes dentro de la Intranet ya que para el desarrollo se a tomado en cuenta a todas las personas que estarán involucradas en la migración.

Otro ventajas del proyecto es que ampliará el conocimiento acerca de la nueva tecnología dentro de la institución especialmente dentro del área de sistemas y lo que es más importante dentro de los estudiantes de la Facultad de Sistemas e Informática que son la parte más importante dentro de la institución y por ende merecen estar actualizados.

I Etapa de Información y motivación

Esta etapa consiste básicamente en tres fases, la realización de “Encuestas”, “Entrevistas” y una “Información Básica” hacia los involucrados en el proceso de la migración.

Como involucrados en el proceso de migración o lo que vamos a llamar nuestro “Universo de Investigación” tenemos tres grupos que se dividen en:

1. **Departamento de Organización y Sistemas:** Ya que son los encargados de la Administración y Soporte de todo lo que comprende la Intranet de la ESPE-L , sus tareas Informáticas y de Sistemas. El total de personal dentro de este departamento es de cinco (5) personas.
2. **Profesores de la Facultad de Sistemas e Informática**: Los profesores tomados en cuenta en este punto, son los que tienen los conocimientos respectivos dentro del área de sistemas; refiriéndonos exactamente Ingenieros en Sistemas ya que estos, dentro de la Facultad son los que dictan las materias de especialidad y están en la capacidad de aportar con conocimientos y experiencia dentro del proceso. El número profesores que se encuentran en el grupo de adquisición de información es de seis (6) profesores Ingenieros en Sistemas.
3. **Alumnos de la Facultad de Ingeniería en Sistemas e Informática**: Para seleccionar quien entra en este grupo se tomo en cuenta la Malla Curricular de la Facultad de Sistemas e Informática, y según está, los aptos son los alumnos de Quinto, Sexto, Séptimo, Octavo y Noveno Nivel de la misma; ya que este grupo poseen conocimientos de Comunicación de Datos y Redes que es lo esencial para la investigación. El total de alumnos que se tomo en cuenta para esta etapa es de veinte y tres (23) alumnos.

1.1 ENCUESTAS

La primera fase dentro de la Etapa de Información y Motivación son las “encuestas” las cuales son dirigidas a los tres grupos que conforman nuestro “universo de investigación”; cabe destacar que estos son: Personal del área de Organización y Sistemas, Grupo de Ingenieros y alumnos de la Facultad de Sistemas que cumplen con los requisitos antes ya descritos.

El objetivo de las encuestas es saber que tan informados están los tres grupos sobre los temas seleccionados; cabe destacar que estos temas son de conocimiento básico y al igual están divididos en tres partes; ya que cada una de ellas se refiere a un tema en especial.

Los temas que de la encuesta son:

Primer bloque de preguntas

- Conocimiento básicos del Protocolo TCP/IP.

Segundo bloque de preguntas

- Conocimientos básicos del Protocolo IPv6 y Técnicas de Migración.

Tercer bloque de preguntas

- Está enfocado hacia la implantación del protocolo IPv6 en la ESPE-L y su por que.

De la misma manera los resultados se clasificaron en tres bloques y se obtuvo sus porcentajes por medio de gráficos de barras.

Teniendo en cuenta que los conocimientos por parte de los Docentes de Organización y Sistemas, Ingenieros y alumnos de la Facultad de Sistemas e Informática no son los mismos para una mejor comprensión se la dividió por grupos; los mismos grupos ya antes divididos dentro de nuestro universo de investigación.

A continuación los resultados de las encuestas:

- **Primera bloque de preguntas de la encuesta**

Son conocimientos básicos sobre el protocolo TCP/IP o IPv4 como:

Clases de red o direcciones y tamaño de la dirección TCP/IP, tipo de enrutamiento de TCP/IP y desventajas que presenta el TCP/IP o Protocolo IPv4.

Se lo realizo en el orden jerárquico descrito antes:

1.- Departamento de Organización y Sistemas

Son dirigidas hacia todos los administrativos del departamento de Organización y Sistemas exactamente cinco personas son los que conforman este; cada barra representa una pregunta con su respectivo porcentaje, tomando 100% significa que existe un total dominio del tema.

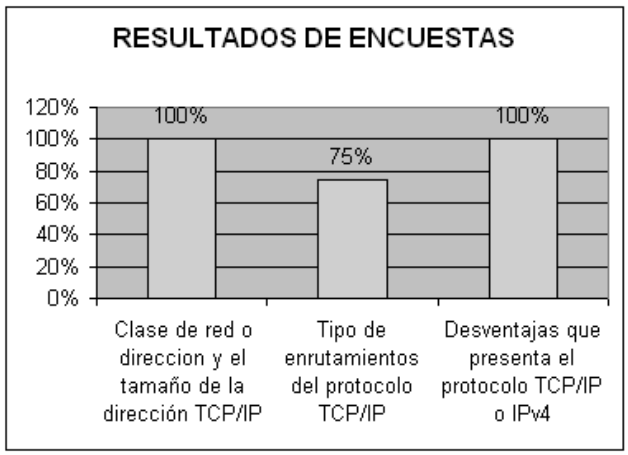


Gráfico 3.1: Resultado sobre los conocimientos básicos de TCP/IP a Organización y Sistemas

Como resultado se obtuvo: en la primera pregunta se un 100% lo cual significa que todo el personal que labora en el departamento conoce sobre clases de redes y su tamaño con respecto al protocolo TCP/IP, en la segunda barra obtuvimos 75% lo cual significa que la mayoría sabe los tipos de enrutamiento del protocolo TCP/IP

y en la tercera pregunta el 100% representa que también conocen sobre las desventajas que presenta el protocolo.

Tomando en cuenta los porcentajes obtenidos, que son altos, se concluye que del total de personas encuestadas en Organización y Sistemas posee alto grado de conocimientos y dominio sobre el protocolo TCP/IP.

2.- Profesores de la Facultad de Sistemas e Informática:

Fueron dirigidas al grupo seleccionado dentro de los profesores de la Facultad de Sistemas, y cada barra representa una pregunta con su respectivo porcentaje, tomando 100% significa que existe un total dominio del tema.

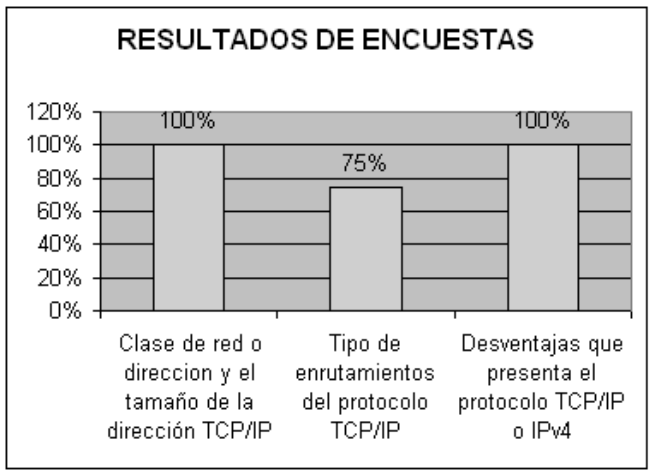


Gráfico 3.2: Resultado sobre los conocimientos básicos de TCP/IP a los Ingenieros en Sistemas de la Facultad de Sistemas

El resultado fue en la primera pregunta 100% lo cual significa que los Ingenieros de la Facultad de Sistemas encuestados tienen un conocimiento completo sobre clases de redes y su tamaño con respecto al protocolo TCP/IP, la segunda barra se obtuvo 75% lo cual significa que la mayoría sabe sobre los tipos de enrutamiento

del protocolo TCP/IP y en la tercera pregunta el 100% representa que también conocen sobre las desventajas que presenta el protocolo.

Los porcentajes obtenidos como podemos ver son altos, y se concluye que los Ingenieros de la Facultad de Ingeniería en Sistemas tienen un alto grado de conocimientos y dominio sobre el protocolo TCP/IP.

3.- Alumnos de la Facultad de Ingeniería en Sistemas e Informática:

Las encuestas se realizaron hacia el grupo de alumnos seleccionados que cumplen con los requisitos ya antes mencionados de acuerdo a la malla curricular.

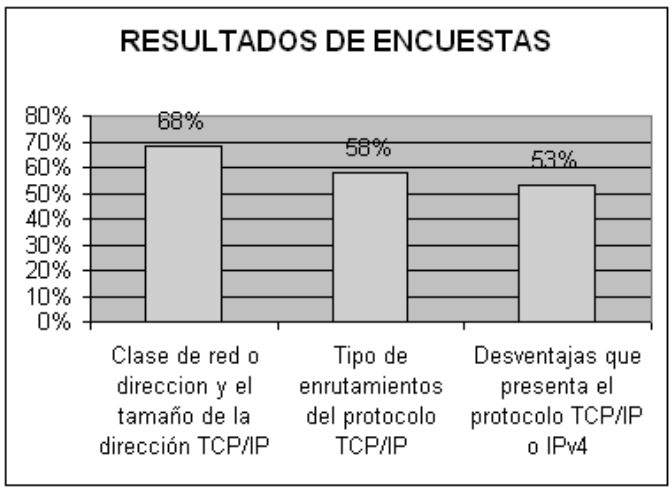


Gráfico 3.3: Resultado sobre los conocimientos básicos de TCP/IP a los alumnos de la Facultad de Sistemas

El resultado que se obtuvo en la primera pregunta es 68% lo cual significa que no se tiene un dominio total sobre el tema de clases de redes y su tamaño con respecto al protocolo TCP/IP lo que representa un poco menos de la mitad de alumnos que no conocen el tema y siendo un aspecto básico se debería obtener un

resultado más alto. En la segunda barra obtuvimos 58% lo cual significa que la mitad del grupo de alumnos encuestados conocen sobre los tipos de enrutamiento del protocolo TCP/IP al igual que en la tercera pregunta que se obtuvo 53% que al igual es un porcentaje medio sobre las desventajas que presenta el protocolo.

Tomando en cuenta los porcentajes obtenidos, en las pregunta se puede decir que son favorables, ya que dentro del grupo de alumnos encuestados están los alumnos de quinto y sexto nivel y ellos de acuerdo a la malla curricular tienen conocimientos básicos que se refleja en la primera pregunta y conocimientos medios o escasos en la segunda y tercera; mientras que los de séptimo, octavo y noveno fueron favorables ya que poseen más dominio del tema sobre redes, por lo que en la gráfica presentan porcentajes medios.

- **Segunda bloque de preguntas de la encuesta**

Al igual son conocimientos básicos de del Protocolo IPv6 y Técnicas de Migración

1.- Departamento de Organización y Sistemas

Al igual que en el primer bloque los administrativos del departamento de Organización y Sistemas contestaron las siguientes preguntas y se obtuvo los siguientes resultados; cada barra representa una pregunta con su respectivo porcentaje, tomando 100% significa que existe un total dominio del tema.

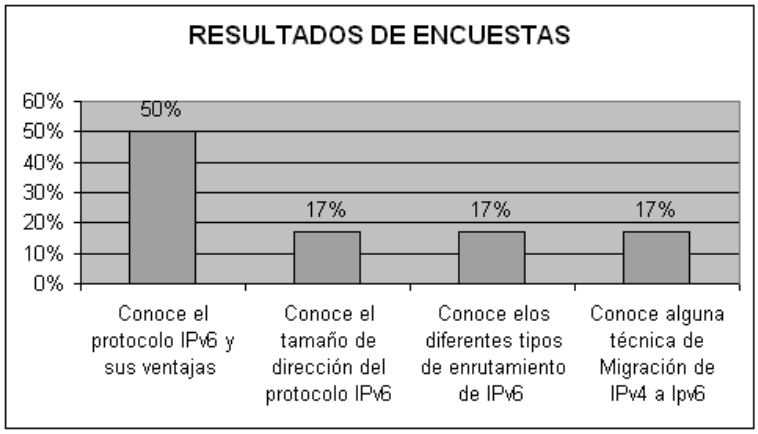


Gráfico 3.4: Resultado sobre los conocimientos básicos del protocolo IPv6 a Organización y Sistemas

El 50% de la primera barra significa que la mitad del personal que labora dentro de este departamento tiene un conocimiento medio, en la segunda, tercera y cuarta barra se puede observar un 17% que representa una cifra muy baja; teniendo en cuenta que las tres barras representan a preguntas más complejas que la primera. por tanto se obtuvo como resultado que el personal que conforma Organización y Sistemas tiene un conocimiento muy escaso del protocolo IPv6 y sus características.

2.- Profesores de la Facultad de Sistemas e Informática:

Fueron dirigidas al grupo seleccionado dentro de los profesores de la Facultad de Sistemas, y cada barra representa una pregunta con su respectivo porcentaje, tomando 100% significa que existe un total dominio del tema.

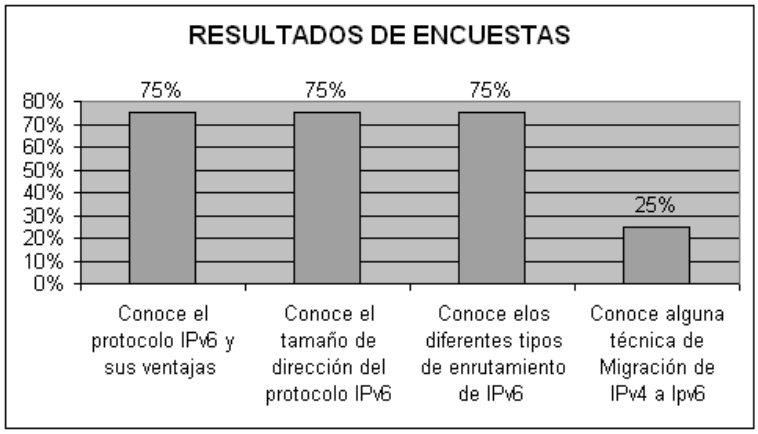


Gráfico 3.5: Resultado sobre los conocimientos básicos del protocolo IPv6 a Ingenieros en Sistemas de la Facultad de Sistemas

El resultado en la primera, segunda y tercera pregunta es 75% lo que se puede concluir que se tiene docentes actualizados con respecto a la nueva tecnología en un porcentaje aceptable mientras que con respecto al conocimiento de técnicas de migración o cuarta barra es de 25% lo que se puede decir que es escaso tomando en cuenta que este tema es muy importante.

Los porcentajes obtenidos como podemos ver son aceptables, y se concluye que los Ingenieros de la Facultad de Ingeniería en Sistemas tienen un grado de conocimientos y dominio sobre el protocolo IPv6.

3.- Alumnos de la Facultad de Ingeniería en Sistemas e Informática:

Las encuestas se realizaron hacia el grupo de alumnos seleccionados que cumplen con los requisitos ya antes mencionados de acuerdo a la malla curricular.

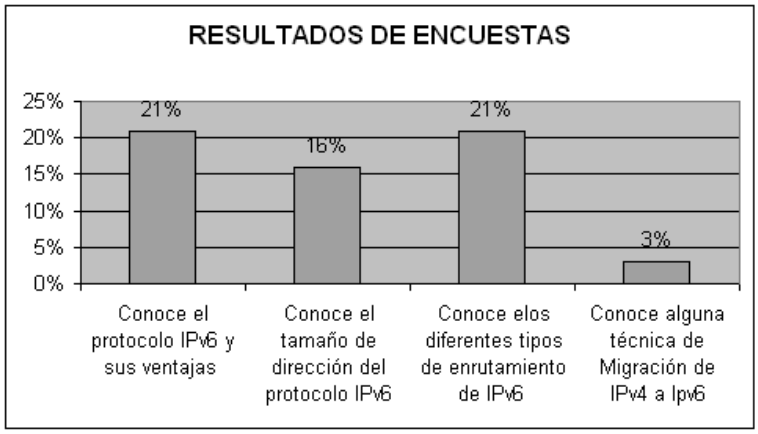


Gráfico 3.6: Resultado sobre los conocimientos básicos del protocolo IPv6 a los alumnos de la Facultad de Sistemas seleccionados

El 21% refleja un porcentaje muy bajo ya que teniendo en cuenta que la primera barra representa el conocimiento básico del protocolo IPv6, el 16% de la segunda barra, 21% y 3% son preguntas mucho más complejas y al igual que la primera barra son resultados que representan escasos conocimientos, lo cual es crítico ya que, teniendo en cuenta que los estudiantes deben estar actualizados sobre las nuevas tecnologías ya sea por si mismos o por la parte académica.

- **Tercer bloque de preguntas de la encuesta**

Está enfocado hacia la implantación o la migración hacia el protocolo IPv6 en la intranet de la ESPE-L

A continuación los resultados obtenidos en las encuestas:

1.- Departamento de Organización y Sistemas

Son dirigidas hacia todos los administrativos del departamento de Organización y Sistemas; cada barra representa una pregunta con su respectivo porcentaje, tomando 100% significa que existe un total dominio del tema.

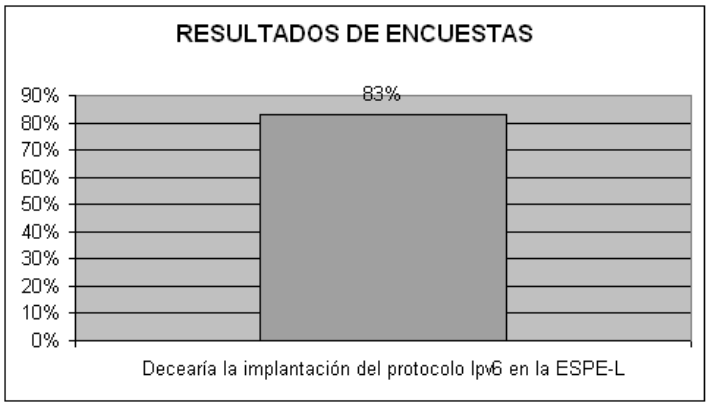


Gráfico 3.7: Resultado sobre el planteamiento de implantación del protocolo IPv6 a Organización y Sistemas

El 83% de los docentes que integran el departamento de organización y sistemas desearían una implantación del protocolo IPv6 ya que aportaría a los servicios que ellos desempeñan.

2.- Profesores de la Facultad de Sistemas e Informática:

Fueron dirigidas al grupo seleccionado dentro de los profesores de la Facultad de Sistemas, y cada barra representa una pregunta con su respectivo porcentaje, tomando 100% significa que existe un total dominio del tema.

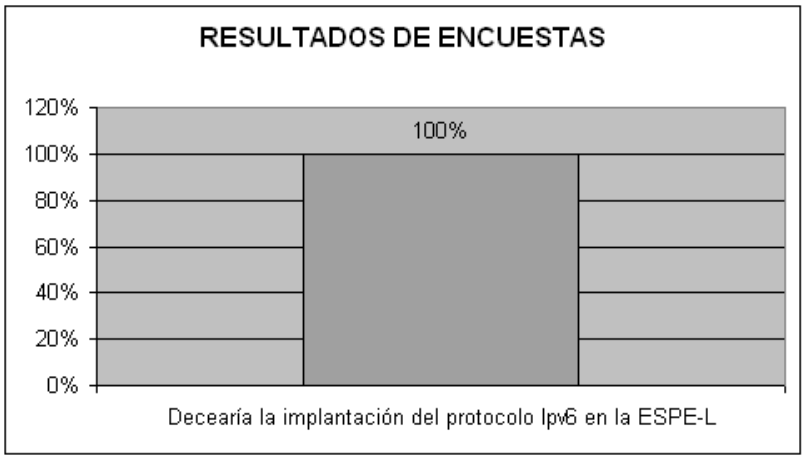


Gráfico 3.8: Resultado sobre el planteamiento de implantación del protocolo IPv6 a Ingenieros en Sistemas de la Facultad de Sistemas

Con el 100% que se obtuvo en esta pregunta se aprecia que los docentes están totalmente interesados en la implementación del protocolo ya que aportaría mucho a sus conocimientos.

3.- Alumnos de la Facultad de Ingeniería en Sistemas e Informática:

Las encuestas se realizaron hacia el grupo de alumnos seleccionados que cumplen con los requisitos ya antes mencionados de acuerdo a la malla curricular.

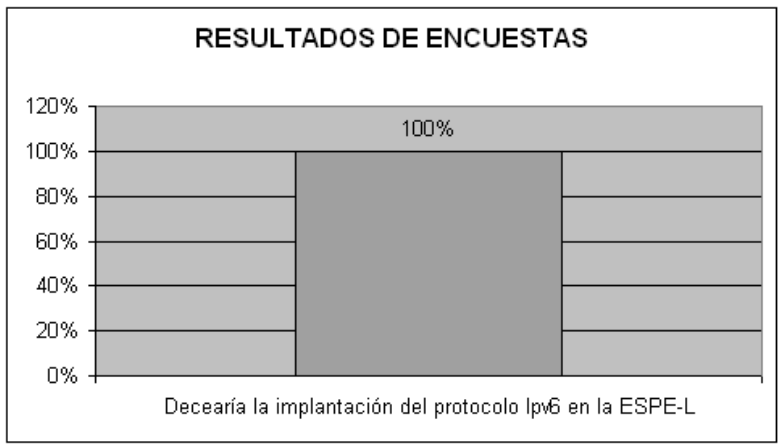


Gráfico 3.9: Resultado sobre el planteamiento de implantación del protocolo IPv6 a alumnos de la Facultad de Sistemas seleccionados

Al igual que profesores, los alumnos también están totalmente de acuerdo en la implementación; el 100% lo refleja y es un buen resultado ya que los estudiantes presentan interés.

1.2 ENTREVISTAS

Las Entrevistas fueron realizadas hacia dos grupos importantes dentro de la ESPE sede Latacunga y de la Facultad de Sistemas, como el Departamento de Organización y Sistemas y a los profesores de la Facultad de sistemas e informática y con conocimientos en esta área; teniendo un total de once (11) personas, realizándose preguntas básicas sobre posibles problemas obtenidos con el protocolo TCP/IP o IPv4, acerca de conocimientos básicos del protocolo de IPv6 como las ventajas que presentaría al ser implantado en la institución, beneficios que presentaría al departamento o a hacia cada persona dentro de su área de trabajo, y más que todo nos permitió saber si la parte ejecutiva está al tanto de la posible migración ya que algún momento está tecnología será indispensable para la institución, y como dentro de lo más importante son saber las expectativas con relación al uso del nuevo protocolo.

Dentro de los resultados en los profesores se pudo obtener como conclusiones que al momento no han tenido problemas con el protocolo IPv4 ya que en el área en la que ellos se encuentran no están en contacto con este, pero tienen conocimientos básicos sobre el tamaño y ventajas que este presenta y al mismo tiempo desconocen sobre alguna técnica de migración o si en alguna empresa dentro del país está empleando este protocolo, y al mismo tiempo presentan interés por conocer más sobre el tema; En conclusión todos están de acuerdo con conocer

más sobre está tecnología ya que presenta muchos beneficios, es de actualidad y está muy cercana su implementación.

El resultado que se obtuvo dentro del Departamento de Organización y Sistemas fue más claro ya que están en contacto continuo con la administración de la red de la Institución, Aquí se tienen en cuenta que se encuentra divididos en cuatro área específicas como: Administración de los Servicios Administrativos, Aplicaciones cliente/servidor, Laboratorios de Internet, y el Área más importante dentro de la institución y del proyecto que es el Área de Redes.

La mayoría del personal no administra la red, ya que cada uno se encarga de las áreas ya mencionadas, pero poseen conocimientos sobre el protocolo, al igual que las ventajas que este nos brinda; Sobre técnicas de migración sus conocimientos fueron muy escasos y con relación a si alguna institución emplea estos también fueron escasos, pero todos están de acuerdo que la tecnología nueva aportaría a la institución con el aumento seguridades y beneficios para todos los que conforman la institución.

Sobre el área de redes que es lo más importante dentro del proyecto la persona encargada posee los conocimientos necesarios sobre tamaño, ventajas pero muy pocos sobre técnicas de migración al igual que de configuración y puesta en marcha.

Por el momento no se ha tenido que realizar actualizaciones ni uso de parches en el protocolo TCP/IP ya que básicamente la red es administrada desde la ESPE MATRIZ y esta se encarga de la administración hacia todos las sedes.

En cuanto a actualizaciones se han realizado de Sistemas Operativos y Software para ir mejorando e ir acorde a la tecnología y a las necesidades que la Escuela va presentando.

El Departamento de sistemas tampoco a presentado algún inconveniente con el protocolo ya que como antes ha sido mencionado el Internet es subministrado desde

la Matriz, Area de Internet o mediante conexión Dial up por el proveedor de Andinanet siendo esta conexión local. Además que todo servicio que la facultad la requiera es directamente administrado por el área de redes.

1.3 EXPLICACION BASICA

Luego de haber realizado las encuestas y entrevistas a todo el personal Administrativo, profesores y alumnos se hizo una explicación breve de sobre el protocolo IPv6, como las ventajas, desventajas, principal problema de IPv4, el por que aparece el nuevo protocolo IPv6 y como podemos migrar mediante los diferentes tipos que este nos presenta.

La explicación fue básicamente personalizada ya que luego de la encuesta presentaron incógnitas e inquietud por saber sobre el tema "protocolo IPv6".

Por parte de la mayoría de los administrativos y profesores el tema ya era conocido pero en un aspecto básico y se logro aclarar las dudas y esclarecer sus conocimientos.

Por parte de los alumnos que casi la mayoría ignoraba del nuevo protocolo se tubo gran inquietud por conocer más, lo mismo que se realizo la explicación de todos los servicios y de lo que básicamente es el protocolo IPv6.

Los alumnos quedaron satisfechos con la explicación y al mismo tiempo expusieron que necesitarían que dentro del área de redes existiera un estudio más profundo, ya que es tecnología nueva, útil y que actualmente se esta utilizando y sobre todo es un tema de actualidad dentro de nuestra área.

II Etapa de Definición de Visión y Objetivos

2.1 Visión

Obtener una red Eficiente y Segura empleando el protocolo IPv6; permitiendo aprovechar al máximo todas las ventajas que este nos brinda; y a la vez familiarizar tanto a Docentes como alumnos de la Facultad de Sistemas.

2.2 Objetivos

1. Incorporar el protocolo IPv6 dentro de la Intranet de la ESPE-L
2. Impulsar a la investigación y desarrollo de aplicaciones sobre el protocolo IPv6
3. Vincular a la comunidad Politécnica con la nueva tecnología.
4. Emplear los servicios que brinda IPv6
5. Brindar satisfacción personal al estar actualizado tecnológicamente.
6. Utilizar aplicaciones con soporte IPv6.
7. Permitir conocer y realizar pruebas a los alumnos de la Facultad de Ingeniería en Sistemas.

III Etapa de Estudio de la Organización (Intranet de la ESPE-L)

Está etapa se la puede llamar básicamente como la etapa de Inventario tanto de Hardware como de Software ya que se estudia toda la estructura de la red de la ESPE-L y determinará que se deberá cambiar o actualizar para llegar a la migración y/o coexistencia con el protocolo IPv6.

A continuación se presenta la información sobre el Hardware y Software que posee la Escuela Politécnica del Ejercito sede Latacunga, la misma que se la a dividido por áreas y/o departamentos y al mismo tiempo se irá detallando la importancia de esta en forma individual y la influencia dentro de la administración de la red.

La red de la ESPE-L es una red LAN y esta conectada a la red principal de la ESPE Matriz formando una WAN ya está esta tiene varias extensiones como ESPE IDIONAS en QUITO; IASA SANGOLQUI Y IASA SANTO DOMINGO.

La RED LAN de la ESPE Latacunga, consta de Servidores, Terminales, Conmutadores y Concentradores, Modems, Router y cables de red, Sistemas Operativos, Software de Aplicación que serán descritos a continuación; esta red para una mejor comprensión y facilidad de control se la a dividido de la siguiente forma:

1. RED ACADEMICA
2. RED ADMINISTRATIVA

3.1 RED ACADEMICA

Dentro de la Red Académica se encuentra los laboratorios de la Facultad de Sistemas e Informática, los laboratorios de Computación para uso de las otras Facultades y el Departamento de control de laboratorios.

Esta red consta de siete laboratorios como: Multimedia, Novel, Unix, Redes, Micros 1, Micros 2, Sistemas Digitales que a continuación son detalladas una a una.

√ **MULTIMEDIA**

Nº PC y Procesador	20 Pentiun II
Memoria	128 RAM
Disco Duro	10 GB
Nº Servidores	1 con S.O. Linux 9.0 y 2000 Server

Nº HUB	1 Dual Speed 10/100 Mbps
Nº Switc	1 SW 10/100 Mbps
MODEM	Kbps
Tipo de cable	UTP CATEGORIA 5E blindado
Conectores	RJ 45
Nº NIC	20 NICs Ethernet 10Mbps
Software	Windows 98, Linux 7.0.
Observaciones	Uso para la Facultad de Sistemas

Tabla 3.1: Equipos dentro del laboratorio Multimedia

√ **NOVEL**

Nº PC y Procesador	20 Pentiun IV
Memoria	256 RAM
Disco Duro	60 GB
Nº Servidores	1 con S.O. Linux 9.0
Nº HUB	1 Dual Speed 10/100 Mbps
Nº Switc	NINGUNO
MODEM	56 Kbps
Tipo de cable	20 inalambricos
Conectores	Inalambrico
Nº NIC	20 NICs Ethernet dual speed 10/100Mbps
Software	Windows 98, Linux 7.0.
Observaciones	Uso para la Facultad de Sistemas

Tabla 3.2: Equipos dentro del laboratorio Novel

√ **UNIX**

Nº PC y Procesador	12 Pentiun II
Memoria	128 Mbps
Disco Duro	10 GB

Nº Servidores	1 Servidor IBM
Nº HUB	1 Dual Speed 10/100 Mbps
Nº Switc	NINGUNO
MODEM	56 Kbps
Tipo de cable	UTP CATEGORIA 5E blindado
Conectores	RJ 45
Nº NIC	12 NICs Ethernet de 100Mbps
Software	Windows 98
Observaciones	Uso para todas las Facultades

Tabla 3.3: Equipos dentro del laboratorio Unix

√ **REDES**

Nº PC y Procesador	12 DTK Pentiun MMX
Memoria	64 RAM
Disco Duro	10 Gb
Nº Servidores	NINGUNO
Nº HUB	1 Dual Speed 10/100 Mbps
Nº Switc	NINGUNO
MODEM	56 Kbps
Tipo de cable	UTP CATEGORIA 5E blindado
Conectores	RJ 45
Nº NIC	12 NICs Ethernet dual speed 10/100Mbps
Software	Windows 98
Observaciones	Uso para todas las Facultades

Tabla 3.4: Equipos dentro del laboratorio de Redes

√ **MICROS 1**

Nº PC y Procesador	15 Pentiun 3
Servidor	NINGUNO

Memoria	128 RAM
Disco Duro	40 GB
Nº Servidores	NINGUNO
Nº HUB	1 Dual Speed 10/100 Mbps
Nº Switc	NINGUNO
MODEM	56 Kbps
Tipo de cable	UTP CATEGORIA 5E blindado
Conectores	RJ 45
Nº NIC	15 NICs Ethernet de 100Mbps
Software	Windows 98, Visual Basic, Autocad, Oficce
Observaciones	Uso para todas las Facultades

Tabla 3.5: Equipos dentro del laboratorio Micros 1

√ **MICROS 2**

Nº PC y Procesador	6 P3, 3 Mediun Tower, 5 Compak 486, 1 Clon P1
Servidor	NINGUNO
Memoria	256,128 ,64 RAM
Disco Duro	60 GB,8 GB
Nº HUB	NINGUNO
Nº Switc	NINGUNO
MODEM	56 Kbps
Tipo de cable	UTP CATEGORIA 5E blindado
Nº NIC	15 NICs Ethernet 100Mbps
Software	Windows 98, Visual Basic, Autocad, Oficce
Observaciones	Uso para todas las Facultades

Tabla 3.6: Equipos dentro del laboratorio Micros 2

√ **SISTEMAS DIGITALES**

Nº PC y Procesador	15 Pentiun 4 de 1.4

Servidor	NINGUNO
Memoria	256 RAM
Disco Duro	60 GB
Nº Servidores	NINGUNO
Nº HUB	1 Dual Speed 10/100 Mbps
Nº Switc	NINGUNO
MODEM	56 Kbps
Tipo de cable	UTP CATEGORIA 5E blindado
Conectores	RJ 45 y Puertos USB
Nº NIC	15 NICs Ethernet dual speed 10/100Mbps
Software	Windows 98
Observaciones	Uso para todas las Facultades

Tabla 3.7: Equipos dentro del laboratorio Sistemas Digitales

√ **OFICINA**

Este departamento se encarga de organizar, controlar y actualizar los laboratorios y horas disponibles; a demás de brindar servicios a los estudiantes para prácticas y tareas.

A continuación se detalla los equipos que se encuentran en la oficina de administración de laboratorios.

Nº PC y Procesador	4 Pentiun II

Servidor	1 Servidor con dos HD
Servidor HD 1	Con sistema Operativo Linux 9.0
Servidor HD 2	Con sistema Operativo 2000 Server
Memoria	256 RAM
Disco Duro	60 GB
Nº HUB	1 Dual Speed 10/100 Mbps
Nº Switch	1 SW
MODEM	128 Kbps
Tipo de cable	UTP CATEGORIA 5E blindado y Fibra Optica
Conectores	RJ 45
Nº NIC	15 NICs Ethernet 10/100Mbps
Software de PCs	Windows 98
Observaciones	Uso para el personal de Administración de Laboratorios

Tabla 3.8: Equipos dentro de la oficina encargada de los laboratorios

El servidor de esta oficina se encuentra conectado al Departamento de Organización y Sistemas por cable de Fibra Optica para el uso de la red y de Internet y emplea Linux 9.0.

Al momento también posee conexión vía Dial up con el proveedor de Andinanet con conexión de 56 a 128 Kbps.

3.2 RED ADMINISTRATIVA

La red Administrativa es la más grande dentro de la Intranet ya que está compuesta por las siguientes áreas:

√ Área Financiera

- Departamento Financiero

- Pagaduría

√ Área Administrativa

- Dirección
- Subdirección
- Secretaría Académica
- Bienestar Académico
- Adquisiciones

√ Área Académica

- Facultad de Automotriz
- Facultad de Sistemas e Informática
- Facultad de Electrónica
- Facultad de Electromecánica
- Facultad de Ciencias Administrativas
- Instituto de Ciencias Básicas
- Instituto de Idiomas

√ Área de Centro de Datos

- Organización y Sistemas
- Mantenimiento

√ Área de Producción

Cada una de estas áreas están divididas en sub áreas y contienen un determinado número de computadores en cada una de ellas, unidos a la red LAN de Organización y Sistemas.

El Total de PCs dentro de la Red Administrativa es de 71 los cuales están conectados a los servidores para uso de estos y 17 PCs dentro de está red tienen acceso a Internet.

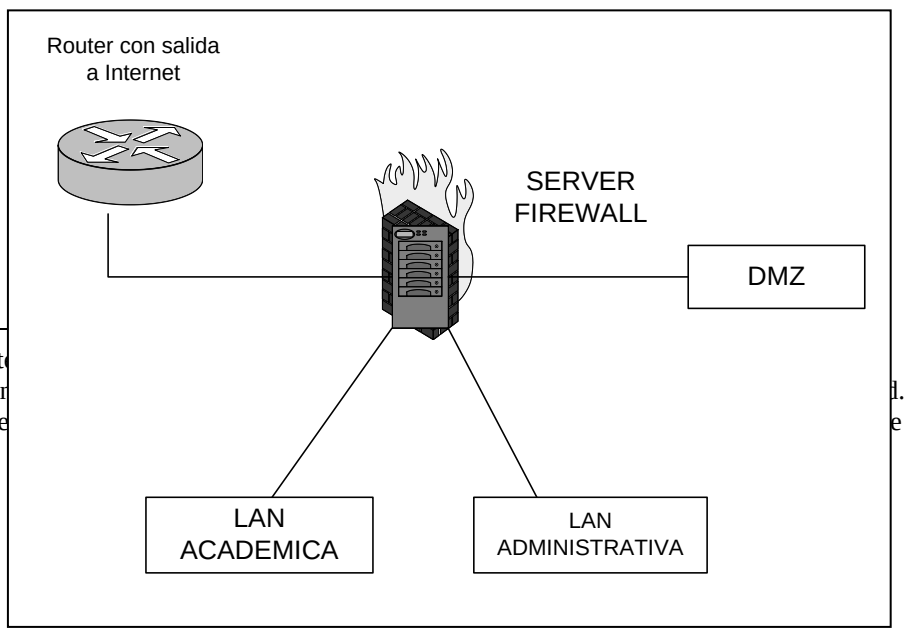
Cada departamento se encuentran con infraestructura tanto física como lógica para tener conexión a Internet; pero generalmente las personas que obtienen este beneficio son Decanos, Subdecanos y Jefes de cada Departamento.

Dentro de cada departamento la conexión a la red es por medio de cable UTP Categoría 5E [81]y con conectores RJ-45 a un HUB y este unido a la red mediante Fibra Óptica.

El Departamento de Producción al igual se encuentra unido al departamento de Centro de Datos por Cable de Fibra Óptica e internamente por cable UTP Categoría 5E.

De una forma simple se puede interpretar a la red de la ESPEL de la siguiente manera:

El firewall[82] está conectado directamente al router, DMZ[83], Red Académica y Red Administrativa.



[81] cable UTP Cat
[82] Firewall.- es u
[83] DMZ .- permite
d.
e su red.

FIGURA 3.1: Estructura de la RED ESPEL simplificada

A continuación se presenta la estructura general de la LAN de la ESPE Latacunga pero de una forma más detallada.

LAN ACADEMICA

Comprende todos los laboratorios de la Facultad de Sistemas y Oficina de Administración de la misma.

Esta posee un servidor con dirección de red 10.2.2 conectada a dos subredes; la primera con un HUB central D-LINK [84]de 24 puertos y la segunda con un Switch para conectarse con los Laboratorios ubicados en la Facultad de Sistemas; El servidor de la oficina de los Laboratorios de Sistemas están conectados al SERVER LINUX FIREWALL, a la RED LAN ADMINISTRATIVA a través de Cable de Fibra Óptica, con acceso a DMZs e INTERNET.

LAN ADMINISTRATIVA

[84] D-LINK.- Marca de un dispositivo HUB

Posee un servidor el cual soporta las siguientes áreas:

- Area Financiera con un Switch Central de 16 puertos marca D-LINK;
- Area Administrativa con Switch Central de 24 puertos marca HP[85];
- Area Academica con un HUB Central de 24 puertos marca D-LINK;
- Area Centro de Datos con un HUB Central de 16 puertos marca D-LINK;
- Area de Producción con un HUB Central de 16 puertos marca D-LINK en el departamento de Organización y Sistemas al cual está unido a través de Fibra Optica a un HUB en producción de 16 puertos marca D-LINK

Toda las áreas están conectada por cable UTP Categoría 5E a excepción del Area de Producción que es por medio de Cable de Fibra Optica.

Tiene la dirección de red 10.2.0 y se encuentra conectada al SERVER LINUX FIREWALL, DMZ LAN ACADEMICA.

DESCRIPCIÓN DE LOS SERVIDORES

La Intranet de la ESPE-L está compuesta por cuatro servidores principales de los cuales cada uno realiza diferente tarea y dos Servidores de Respaldo.

SERVIDORES PRINCIPALES

SERVER NT DE DOMINIO DE DESARROLLO VIRTUAL.- Pertenece a la red académica posee servicio DHCP [86]y es un sitio virtual de desarrollo.

SERVER LINUX FIREWALL.- Servidor principal con FIREWALL trabaja con Sistema Operativo Linux que conecta a las LANs Académica y Administrativa, DMZ y a un router con salida a Internet.

[85] HP.- Marca de dispositivos y PCs
[86] DHCP.- software de servidor que asigna direcciones IP a estaciones de trabajo en una red.

SERVER NT DOMINIO. - Servidor con Sistema Operativo de NT donde se encuentra la base de datos de la Red Administrativa con servicio DHCP.

SERVER 2000 APLICACIONES PRODUCCION.- Servidor con Sistema Operativo 2000 Server y se utiliza para el área de Producción.

SERVIDORES DE RESPALDO

SERVER LINUX RESPALDO.- Es el servidor que se tiene para respaldo del

SERVER LINUX FIREWALL con Sistema Operativo Linux.

BACKUP DOMAIN CONTROL (BDC).- Este es el Servidor de respaldo de los Servidores de la Red Administrativa y Servidor de Producción.

ROUTER.- Se encarga de la interacción e interconexión entre SERVER FIREWALL y a la Red Publica - INTERNET con servicio de ADSL[87] de la ESPE MATRIZ.

DMZ.- Estos se encuentran dentro de dos computadores normales pero hacen el papel de servidor de Correo y servicio WEB.

La red LAN tiene las direcciones de:

10.2.0.0 con mascara 255.255.254.0 Red Administrativa
10.2.2.0 con mascara 255.255.254.0 Red Académica

Todas estas direcciones son protocolo TCP/IP o IPv4.

IV Etapa de elaboración del Plan de Trabajo

[87] ADSL.- Línea de teléfono que transfiere datos a alta velocidad

4.1Hardware a utilizar

De acuerdo al inventario y distribución de la Intranet de la ESPE el numero de máquinas que posee la tecnología necesaria para soportar el protocolo ipv6 es de 56 computadores; y se encuentran dentro del área Académica.

Mientras que las demás seguirán conectadas a la red TCP/IP o IPv4 y se la podrá unir mediante routers con configuración de túnel 6to4 (soporten los dos protocolos); estos se encuentran repartidos en el Area Académica y Administrativa.

Los servidores serán utilizados su totalidad puesto que cubren con la capacidad necesaria para la conexión.

4.2 Sistemas Operativos necesarios para la Implantación

- Sistema Operativos Windows XP con SP1 (Service Pack 1) o SP2 para los host o clientes
- Sistema Operativo Linux Red Hat 9, con Kernel 2.4.x y Bind 9.2 puesto que ya viene con soporte IPv6.

- Parches para Linux como **ipv6calc-0.39**, el cual y se los podrá descargar en: www.bieringer.de/linux/ipv6/ipv6calc/html , y **net-tools** en la dirección ftp://216.254.0.38/linux/freshrpms/redhat/9/yum/yum-2.0.4-1.rh.fr.i386.rpm

- Scrips **IPv6-initscrips-20020125.tar.gz** en la dirección
  www.bieringer.de/linux/ipv6/IPV6-HOWTO/scripts/curren/index.html.

- Service Pach (SP1 o SP2) que se puede descargar o actualizar en la dirección.

"www.microsoft.com/latam/windowsxp/pro/downloads/servicepacks/sp1/default.asp"

- Cable de red RJ45 y Fibra Optica para la conexión entre Host, Servidores, hubs, switch y routers

- Routers Cisco 1700 con capacidad para configuración del protocolo IPv6 el cual posee la capacidad adecuada para montar la intranet.

4.3 Direcciones de Red y mecanismos de Migración

Las direcciones que se utilizarán son las que se autoconfiguran puesto que se podrá hacer uso de "movilidad" y por que son generadas de acuerdo a nuestra dirección MAC.

En cuanto a mecanismos de convivencia se optará por utilizar los túneles ya autoconfigurados, ya que estos nos brindan mucho mas ventajas y seguridad en cuando a la convivencia con los dos protocolos.

Igualmente se podrá tener un servidor con direcciones tanto como IPv4 e Ipv6

V Etapa Instalación y Puesta en Funcionamiento.

5.1Configuración del protocolo IPV6 en diferentes Sistemas Operativos

5.1.1 IMPLEMENTACIÓN DEL PROTOCOLO IPV6 SOBRE MICROSOFT WINDOWS XP

En general, las plataformas de Microsoft disponen de un buen soporte para IPv6, a partir de su versión de Sistema Operativo “Windows XP”, el protocolo viene instalado y su configuración es muy sencilla.

La versión de Windows XP Service Pack 1 ya incluye una implementación de IPv6 lista para instalar.

Para la instalación de IPv6 se requiere del Service Pack 1. Este paquete se obtienen directamente del sitio Web de Microsoft.

“http://www.microsoft.com/windowsxp/downloads/updates/sp1/default.mspx”

Instalación del paquete:

- **SERVICE PACK**

FIGURA 3.2: Inicio del asistente Service Pack 1

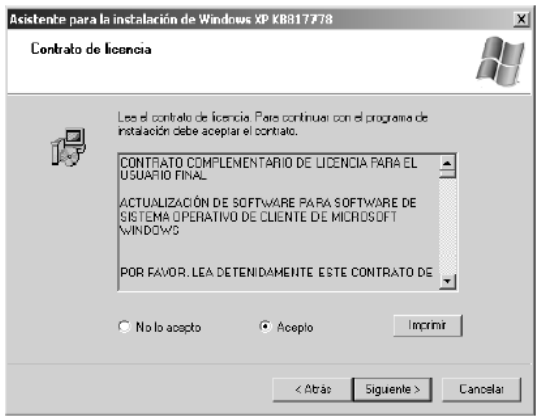


FIGURA 3.3: Cláusulas de Service Pack 1

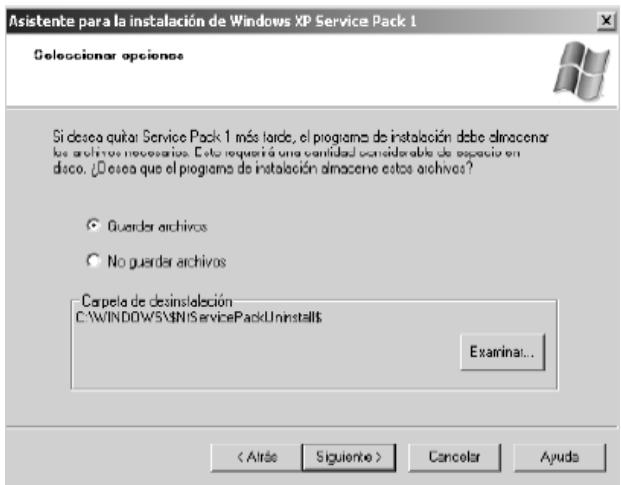


FIGURA 3.4: Ruta de instalación del asistente Service Pack 1

Una vez instalado el paquete procedemos ha configurar el protocolo IPv6 que lo podemos hacer mediante las ventanas de Windows o desde el prompt del sistema

Mediante las ventanas de Windows

Señalamos con el puntero en el icono mis sitios de red y damos un clic con el botón derecho, escogemos en el menú la opción propiedades como podemos observar en la siguiente figura, lo que nos permite configurar los protocolos de red.

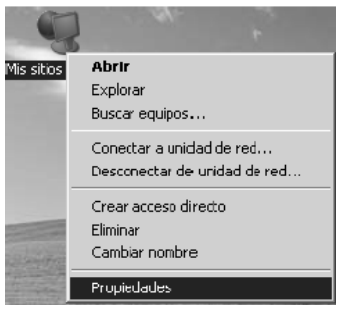


FIGURA 3.5: Propiedades de Mis Sitios de Red

Nos aparece la siguiente pantalla, damos clic derecho en la conexión de are local y seleccionamos en el menú la opción propiedades

FIGURA 3.6: Ingreso a propiedades de Conexión de área local

Aparece la siguiente pantalla

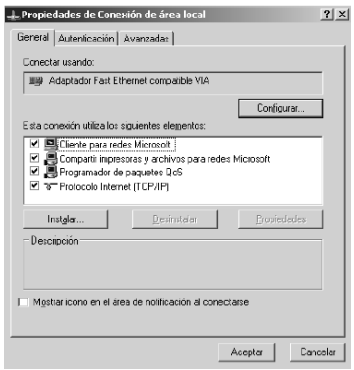


FIGURA 3.7: Propiedades de Conexión de área local

En esta pantalla damos un clic en el botón instalar, elegimos protocolo

FIGURA 3.8: Selección del Tipo de componente de red

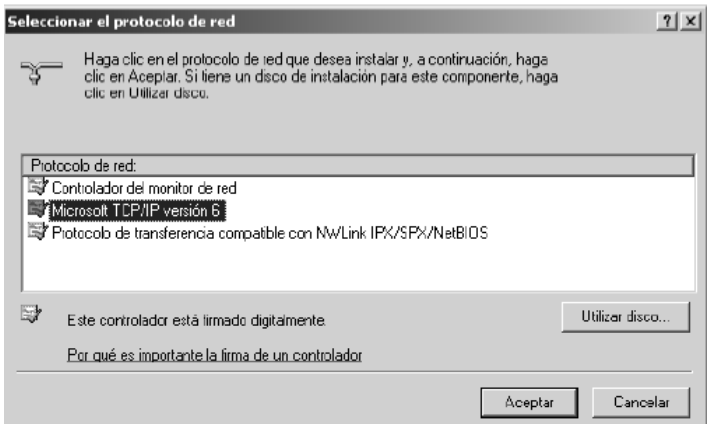


FIGURA 3.9: Selección del protocolo de red IPv6

Seleccionamos Microsoft TCP/IP versión 6 y damos un clic en el botón Aceptar

A continuación podemos observar en que el protocolo IPv6 ha sido instalado.

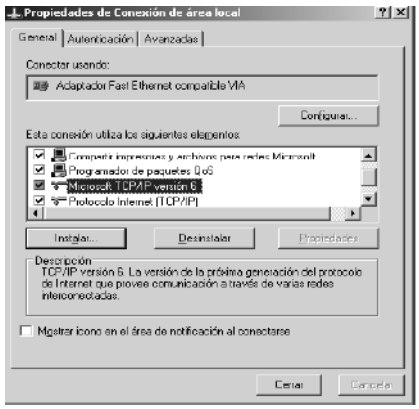


FIGURA 3.10 Protocolo Ipv6 dentro conexiones de área local

Mediante la ventana de Comandos

Otra forma de instalar IPv6 es abrir la ventana de comandos, seleccionamos inicio ejecutar y tecleamos el comando **cmd**

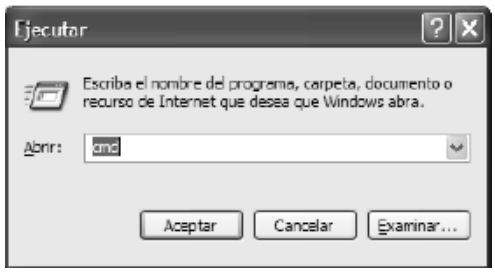


FIGURA 3.11 Ventana de comandos

En la ventana de comandos ejecutamos **"IPV6 install"**

FIGURA 3.12: Instalación correcta del protocolo Ipv6

Aparecerá un mensaje indicando que se ha configurado correctamente. Para comprobar que ha sido correctamente instalado, usar: **Pv6 if**

FIGURA 3.13: Ventana con interfaces de Ipv6

Se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

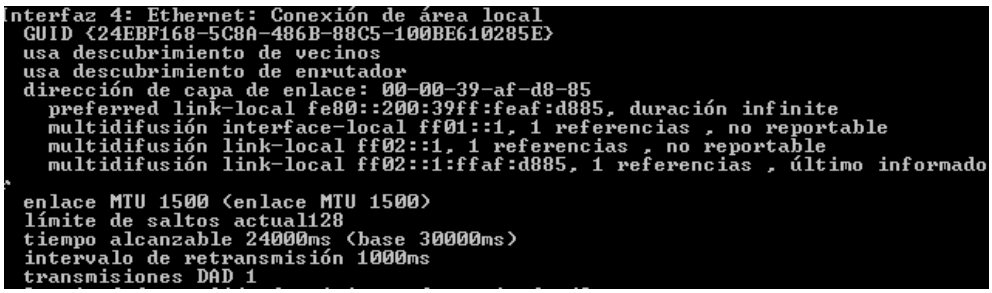


FIGURA 3.14 Dirección Ipv6 en la interfaz de área local

Como podemos ver nuestra **dirección Ipv6 es ... fe80::200:39ff:feaf:d885%4** nos indica que se que se habilito el protocolo IPv6 correctamente

FIGURA 3.15 Direcciones física e Ipv6 en la conexión de área local

Algunos subcomandos requieren privilegios de administrador local. Se puede comprobar el correcto funcionamiento de la pila ipv6 con:

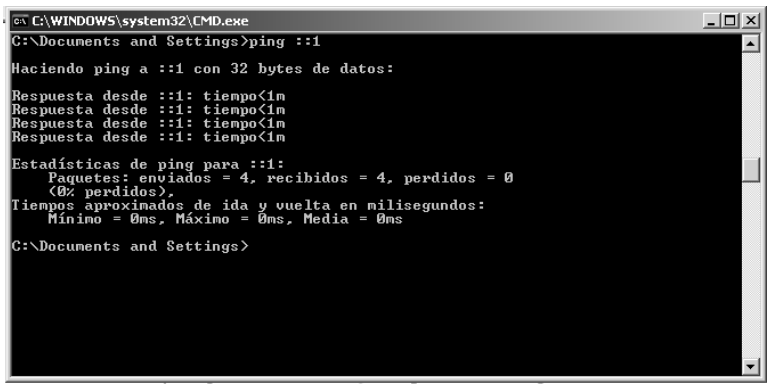


FIGURA 3.16 ejecución del comando ping a dirección loopback IPv6

: :1 es la dirección de loopback en IPv6, al igual que 127.0.0.1 en IPv4. XP incorpora la versión 6 del Internet Explorer, adaptada para navegar en webs IPv6 (e IPv4).

5.1.2 IMPLEMENTACIÓN DEL PROTOCOLO IPV6 SOBRE WINDOWS 2000 SERVER

Previamente para la instalación del protocolo IPv6 en Windows 2000 Server se debe bajar el archivo tpipv6-001205.exe que se encuentra en la dirección:

http://msdn.microsfot.com/downloads/sdks/plataform/tpipv6/download.asp.

Una vez descardado este archivo se lo ejecuta y se crea un directorio con el nombre IPv6TP.

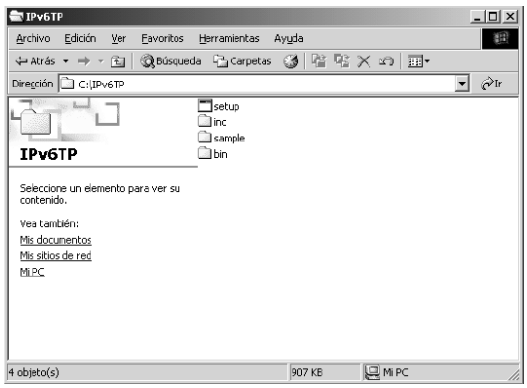


FIGURA 3.17 Archivo parche IPv6

Mediante la ventana de comandos

Para abrir la ventana de comandos en ejecutar tecleamos el comando **cmd**

En el símbolo del sistema ponemos el siguiente comando **Setup.exe –x**

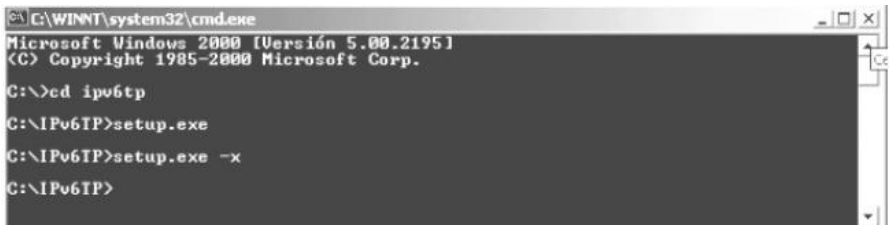


FIGURA 3.18 Instalación del parche en Windows 2000 server

Este comando instala IPv6 en Windows 2000 Server, el protocolo se agrega en entorno de red y queda instalado.

Una vez ejecutada la instalación en la carpeta C:\IPv6TP se crean más archivos que se los pueden ver en el siguiente gráfico, los mismos nos sirven para trabajar con el protocolo.

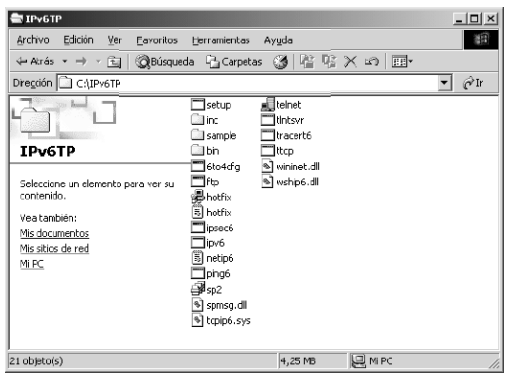


FIGURA 3.19 comandos que presenta archivos parche

Tal como se señaló para Windows XP en Windows 2000 Server se debe agregar el protocolo dentro de entorno de red / propiedades / protocolo / instalar:

Para verificar que IPv6 esta habilitado utilizamos los siguientes comandos.

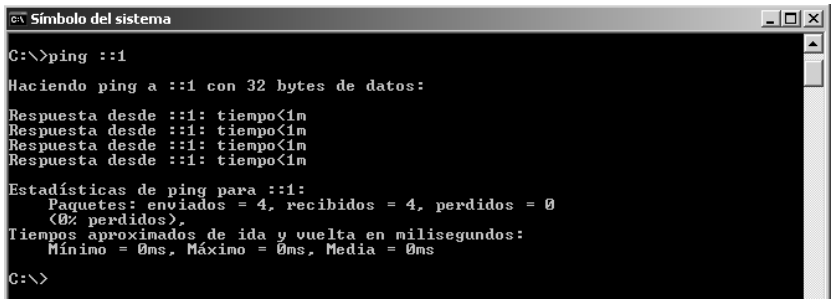


FIGURA 3.20 Dirección loopback IPv6 en Windows 2000 server

Se puede ver que se encuentran habilitadas tanto las interfaces de link, multicast y tunneling

También para verificar la instalación podemos utilizar ping6 a la dirección de loopback

5.1.3 IMPLEMENTACIÓN DEL PROTOCOLO IPV6 SOBRE WINDOWS 2003 SERVER

En Windows 2003, IPv6 ya esta instalado, pero es preciso habilitarlo. Para ello es necesario ejecutar, con privilegios de administrador, el siguiente comando

(Menú de Inicio – Ejecutar – CMD – Enter):

> netsh interface ipv6 install

FIGURA 3.21 Comando de instalación IPv6

Aparecerá un mensaje indicando que se ha configurado correctamente.

También se puede utilizar la interfaz gráfica, seleccionando propiedades sobre la interfaz LAN en la que se desea habilitar IPv6.

Para comprobar que ha sido correctamente instalado, usar:

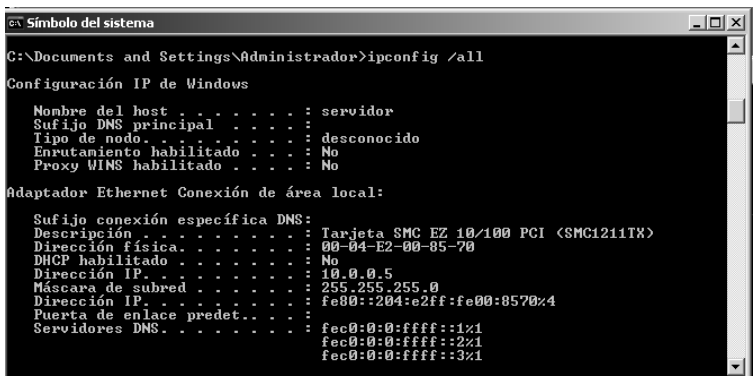


FIGURA 3.22 Direcciones Ipv6 en Windows 2003 server

Se mostrará la configuración y las direcciones IPv6 adquiridas (auto-configuradas) para cada interfaz de red existente.

“netsh interface ipv6” se puede utilizar para comprobar y configurar manualmente interfaces, direcciones y rutas (usuarios avanzados).

Algunos subcomandos requieren privilegios de administrador local. Se puede comprobar el correcto funcionamiento de la pila ipv6 con:

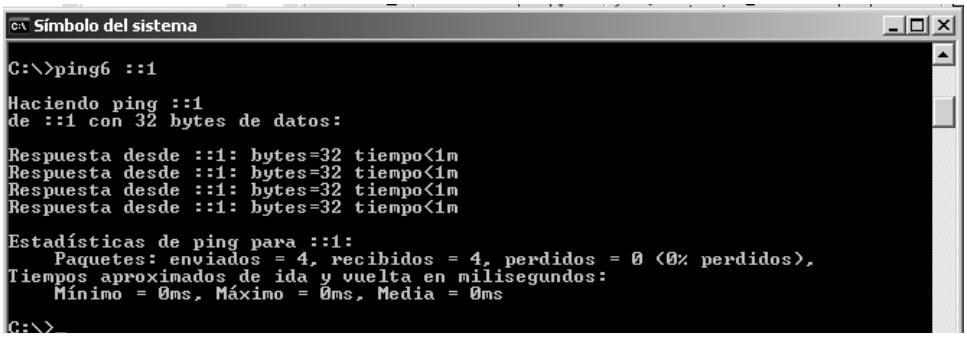


FIGURA 3.23 Direcciones loopback en Windows 2003server

::1 es la dirección de loopback en IPv6, al igual que 127.0.0.1 en IPv4. Windows 2003 incorpora la versión 6 del Internet Explorer, adaptada para navegar en webs IPv6 (e IPv4).

FIGURA 3.24 Comprobación de la configuración de la dirección Ipv6

5.1.4 IMPLEMENTACIÓN DEL PROTOCOLO IPV6 SOBRE LINUX

En linux IPv6 se implementa como un módulo del kernel. Así, las distribuciones con kernel 2.2.x y 2.4.x ya vienen con este soporte y normalmente el módulo IPv6 ya está instalado. De todas formas, habrá que asegurarse que el módulo se carga al arrancar.

Este documento se basa en la distribución Red Hat.

Para comprobar que el kernel soporta IPv6, habrá que comprobar que existe la siguiente entrada:

/proc/net/if_inet6

Si no existe, se puede intentar cargar el módulo ipv6 con:

#> modprobe ipv6

Si se ha cargado correctamente debe existir la entrada mencionada arriba. •

Nota: Descargar el módulo puede, a veces, provocar la caída del sistema. Aunque en versiones actuales de los módulos (kernel 2.4.19 adelante) el soporte es muy estable.

Para que cargue de forma automática el módulo IPv6 cuando se demande, se añade al fichero /etc/modules.conf la siguiente línea:

alias net-pf-10 ipv6
alias sit0 ipv6
alias sit1 ipv6
alias tun6to4 ipv6

Para deshabilitar la carga automática usar alias net-pf-10 off

Paquete net-tools: Usando ifconfig, route. Todas las versiones actuales soportan las extensiones IPv6.

Paquete iproute: Debe existir el programa /sbin/ip, dado que este programa es una extensión del paquete anterior, todas las versiones tienen incorporado el soporte IPv6.

Se utilizan scripts para inicializar todo lo relacionado con IPv6 y para configurar la direcciones v4/v6 de las interfaces. Conviene actualizar a la última versión de los mismos. Estos scripts pueden obtenerse en:

http://www.bieringer.de/linux/IPv6/IPv6-HOWTO/scripts/current/index.html

Aun qué la mayoría de distribuciones actuales configuran estos script en la instalación del sistema.

Se descarga la última versión (IPv6-initscripts-20020125.tar.gz) y se descomprime. •

Se copian los ficheros de script a los directorios correspondientes:

/etc/sysconfig/network-scripts/network-functions-ipv6
/etc/sysconfig/network-scripts/init.ipv6-global
/etc/sysconfig/network-scripts/ifup-ipv6
/etc/sysconfig/network-scripts/ifdown-ipv6
/etc/sysconfig/network-scripts/ifup-sit
/etc/sysconfig/network-scripts/ifdown-sit
/etc/ppp/ip-up.ipv6to4
/etc/ppp/ip-down.ipv6to4
/etc/ppp/ipv6-up
/etc/ppp/ipv6-down
/usr/sbin/test-ipv6-installation
/etc/sysconfig/static-routes-ipv6

Se recomienda instalar ipv6calc para habilitar la detección de direcciones extendidas. Puede obtenerse de:

http://www.bieringer.de/linux/IPv6/ipv6calc/index.html

El tar.gz (ipv6calc-0.39.tar.gz) incluye el fichero spec-file, de forma que se puede crear el RPM mediante:

```
root# rpm –ta ipv6calc-version.tar.gz
```

Para instalar:

```
root# cd /usr/src/redhat/RPMS/i386
root# rpm –i ipv6calc-version.i386.rpm
```

Debe existir, ahora, /bin/ipv6calc

En el fichero sysconfig-ipv6.txt que viene con el paquete de scripts, se da información detallada de los parámetros que se pueden configurar en cada script.

Para comprobar que la configuración es correcta, se puede ejecutar el script:

```
/usr/sbin/test-ipv6-installation
```

Que viene con el paquete.

Configuración de red

Para cambiar el nombre del host se pone en **/etc/sysconfig/network**, la línea:

```
HOSTNAME=nombre_host
```

Conviene, después de esto, añadirlo en el fichero /etc/hosts:

```
::1 nombre_host
```

El nombre de host puede verse en /proc/sys/kernel/hostname, o simplemente ejecutando /bin/hostname sin ningún parámetro.

Se deben añadir entradas en **/etc/hosts** para IPv6:

```
::1 localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
ff02::3 ip6-allhosts
```

Comprobar que en **/etc/protocols/** aparecen:

```
ipv6 41 IPv6
ipv6-route 43 IPv6-Route
ipv6-frag 44 IPv6-Frag
ipv6-crypt 50 IPv6-Crypt
ipv6-auth 51 IPv6-Auth
ipv6-icmp 58 IPv6-ICMP
ipv6-nonxt 59 IPv6-NoNxt
ipv6-opts 60 IPv6-Opts
```

Configurar **/etc/host.conf**:

```
order hosts,bind
multi on
```

De forma que el resolver primero consulte el fichero /etc/hosts y luego al servidor de nombres.

La segunda línea hace que el resolver devuelva todas las direcciones válidas para un host encontrado en /etc/hosts/, en vez de sólo la primera.

Configurar /etc/resolv.conf

cada interfaz existirá un fichero con la configuración que se le asignará al arrancar. Supongamos que se tiene una interfaz hacia la red local (10.0.0.x/24). En **/etc/sysconfig/network-scripts/ifcfg-eth0**

En el script /etc/init.d/network se encuentra:

```
# Add non interface-specific static-routes

if [-f /etc/sysconfig/static-routes]; then
grep “^any” /etc/sysconfig/static-routes | \
        while read ignore args; do
        sbin/route add -$args
done
fi
```

Para asignar a eth0 direcciones IPv6 se realiza lo siguiente:

En el directorio /etc/sysconfig/network-scripts/ habrá un fichero para cada interfaz (eth0).

Se añade:

A ifcfg-eth0 (CASO DE AUTOCONFIGURACIÓN):

```
IPV6INIT=yes # Habilita IPv6 en este interfaz
IPV6AUTOCONF=yes # habilita autoconfiguracion
```

Es esta red se encuentra un router con el RA activado, de forma que la dirección IPv6 se configura automáticamente.

A ifcfg-eth0 (CASO ASIGNACIÓN IPv6 ESTÁTICA):

IPV6INIT=yes # Habilita IPv6 en este interfaz

IPV6AUTOCONF=no # No habilita autoconfiguracion

IPV6ADDR=3ffe:3328:6:2a03::3 # asigna direccion IPv6 fija

A esta interfaz se le asigna una dirección IPv6 fija.

El fichero /etc/sysconfig/network tiene, respecto a IPv6:

NETWORKING_IPV6=yes

IPV6FORWARDING=no

IPV6_AUTOCONF=yes

IPV6_AUTOTUNEL=no

IPV6_DEFAULTGW="3ffe:3328:6:2a03::1%eth0"

Que establece como gateway para IPv6 el router que se conecta por la interfaz eth0.

Mediante ifconfig, comprobar la configuración IPv6.

Cuando se haga un cambio en la configuración de red, se puede reiniciar todo el sistema de red ejecutando el script: /etc/rc.d/init.d/network restart.

Se procede a revisar la configuración de red con el comando siguiente:

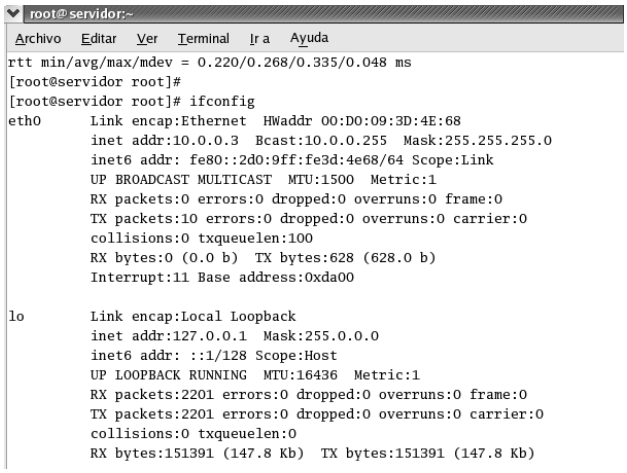


FIGURA 3.25 Dirección Ipv6 en Linux

Como podemos observar en la interfase **eth0** la dirección **fe80::2d0:9ff:fe3d:4e68/64** nos indica que el protocolo IPv6 se habilitó sin ningún inconveniente y en este caso es una dirección de link

Además realizamos las pruebas de ping6 a la dirección de loopback para comprobar la instalación del protocolo.

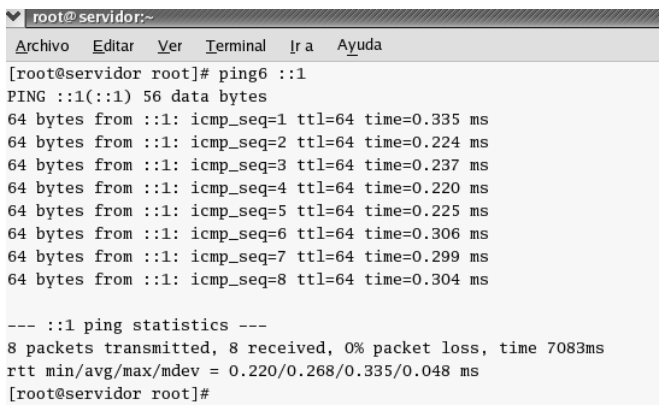


FIGURA 3.26 Dirección loopback en plataforma linux

Donde tenemos las direcciones, lookback (::) y link (FE80)

Comprobando direcciones Ipv6

Para ver la dirección que ha sido autoconfigurada ejecutamos:

#> /sbin/ip -6 addr show dev eth0

#> /sbin/ifconfig eth0

```
[root@servidor root]# /sbin/ifconfig eth0
eth0      Link encap:Ethernet  HWaddr 00:D0:09:3D:4E:68
          inet addr:10.0.0.3  Bcast:10.0.0.255  Mask:255.255.255.0
          inet6 addr: fe80::2d0:9ff:fe3d:4e68/64 Scope:Link
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:628 (628.0 b)
          Interrupt:11 Base address:0xda00

[root@servidor root]# /sbin/ip -6 addr show dev eth0
3: eth0: <BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast qlen 100
    inet6 fe80::2d0:9ff:fe3d:4e68/64 scope link
```

FIGURA 3.27 Dirección Ipv6 en Linux

5.2 Implementación de tunneling

5.2.1.- CONFIGURACIÓN DE TUNNELING MANUAL

Para proveer conectividad con islas ipv6 a través de un túnel 6to4 bajo Linux y usar ipv6 a través de Internet creamos el túnel

Un túnel 6to4 utiliza una máquina que se encarga de entender un tipo especial de paquetes ipv4 que son los paquetes 6to4, estos paquetes encapsulan paquetes ipv6

en paquetes ipv4 y crean un túnel entre nosotros y los sitios que entienden ipv6.

Esto es necesario por que los ISP todavía no ofrecen conectividad ipv6 por lo que por ahora tenemos que emplear túneles

6to4 utiliza un tipo especial de direcciones, una dirección que traduce nuestra dirección pública única ipv4 en una dirección ipv6 única que nos permitirá conectarnos con el broker 6to4 para tener conectividad ipv6.

La dirección 6to4 que nos corresponde se forma utilizando el prefijo 2002: y añadiéndole cada uno de los bytes de nuestra dirección ip ipv4 de dos en dos, en hexadecimal y separados por dos puntos

Este es un script bash que nos ayuda a calcular direcciones ipv6 6to4 a partir de direcciones ipv4:

printf "2002:%02x%02x:%02x%02x::\n" a b c d

Para configurar el túnel tenemos que editar el archivo /etc/network/interfaces, añadiendo las siguientes líneas y utilizando la ip que hemos calculado a partir de la ip publica de nuestra interfaz conectada a internet:

```
ip tunnel add SeisACuatro mode sit ttl 0 remote any local 213.60.102.104
ip link set dev SeisACuatro up
ip −6 addr add 2002:d53c:6668::/16 dev SeisACuatro
ip −6 route add 2000::/3 via ::192.88.99.1 dev SeisACuatro metric 1
```

Lo que creamos en cada línea es lo siguiente:

Creamos el tunel SeisACuatro que encaminará nuestros paquetes 6to4 al broker, le asignamos al túnel nuestra flamante dirección 6to4, y enrutamos cualquier

dirección del rango 2000::/3 a través de la ip anycast del router que nos encaminará al router 6to4 mas cercano a nosotros (::192.88.99.1). En caso de desconfigurar el tunel, hacemos un flush de las rutas añadidas.

Para verificar ejecutamos ifconfig y vemos la interfaz de tunel creada.

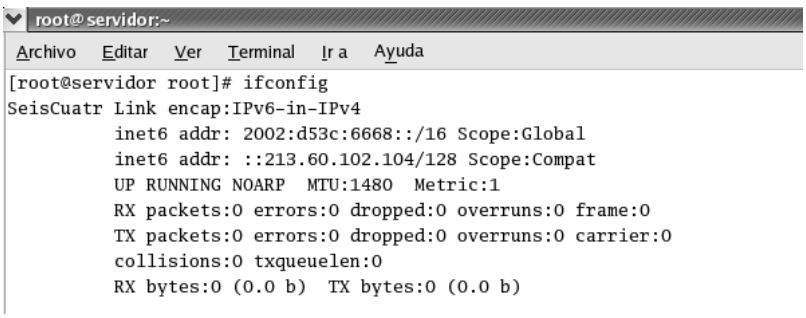


FIGURA 3.28 Túnel creado manualmente

5.2.2.- CONFIGURACIÓN DE TUNNELING AUTOCONFIGURADO

Los tunel configurados es una via simple y rápida para obtener conectividad con ipv6. el cliente necesita instalar y configurar en su PC antes de conectarse al Broker de Migración, El tunel de migración se lo encuentra a través del nombre TSP Client y se lo puede implementar en los siguientes Sistemas Operativos Windows 2000, XP and Server 2003, Linux, FreeBSD, OpenBSD, NetBSD,
VxWorks, QNX, Solaris and Mac OS X

Requisitos:

Tener instalado el protocolo Ipv6

Tener TSP-Client

Intalación de TSP-Client

Para iniciar la instalación de TSP-Cliente damos click en el icono y a continuación seguimos las indicaciones

FIGURA 3.28 Acceso directo a TSP-client

Después de leer la licencia commercial procedemos a dar clik en **I GREE**

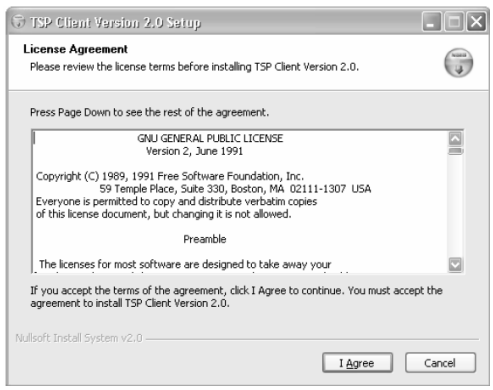


FIGURA 3.29 Cláusulas para la instalación de TSP-Client

Por lo general se requiere instalar TSP binaries y túnel drivers

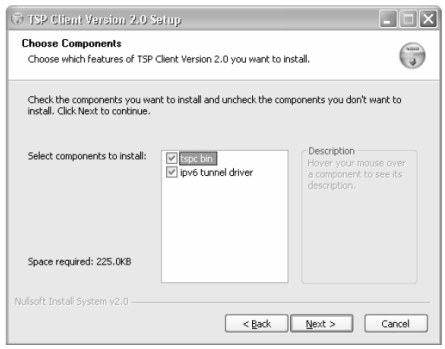


FIGURA 3.30 Archivos de Instalación TSP-Client

Y seguimos con next

Instalamos en el directoria por default

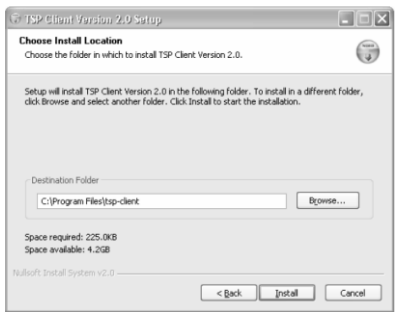


FIGURA 3.31 Directorio de instalacion

Presionamos Continue Anyway

FIGURA 3.32 Instalación del software

a continuación revisamos que la instalación fue completa y exitosamente

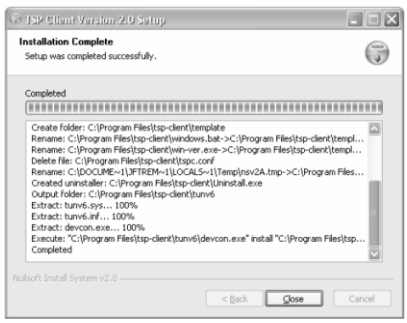


FIGURA 3.33 Comprobación de la instalación

Configuración de TSP-Client

Antes de enpezar con la configuración debemos registrarnos para poder tener acceso al tunel; donde crearemos una cuenta de usuario; podemos registrarnos en http://www.freenet6.net/register.shtml

A continuación vamos al directorio TSP que se encuentra en (C:\Archivos de Programas\tsp-client\) y damos doble clic en el archivo de configuración tsp.config

FIGURA 3.34 Archivo de configuración

Lo abrimos para poder editarlo

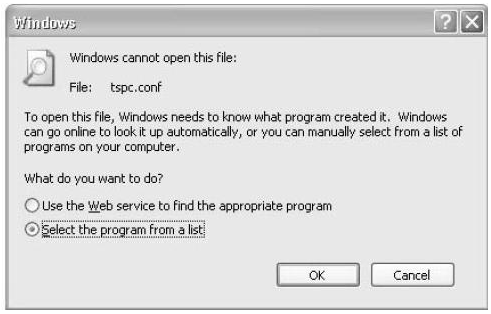


FIGURA 3.35 Programa para editar el archivo TSP comf

A continuación ingresamos el userid y password

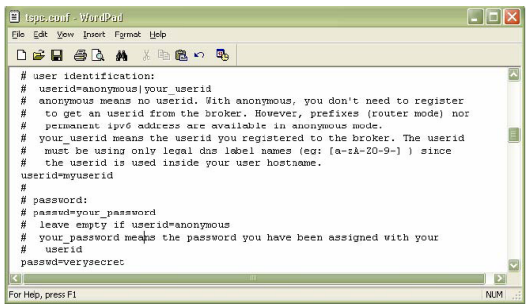


FIGURA 3.36 Configuración del archivo TSP.conf

Guardamos la configuración y cerramos

Luego damos doble click en tspc para ejecutar y aparecera una ventana donde nos aparecera la dirección de cliente asignada por el tunel a nuestro usuario.

FIGURA 3.37 Ejecutamos el cliente

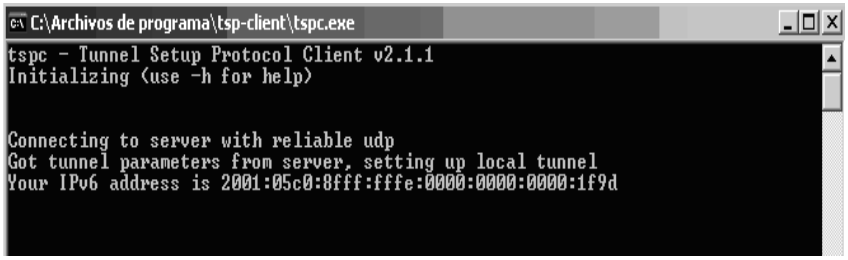


FIGURA 3.38 Conexión al servidor de Internet y asignación de la Dirección IPv6

Probar la conectividad

Para probar la conectividad luego de que el túnel a sido creado comprobaremos el funcionamiento ejecutamos la ventana de comandos

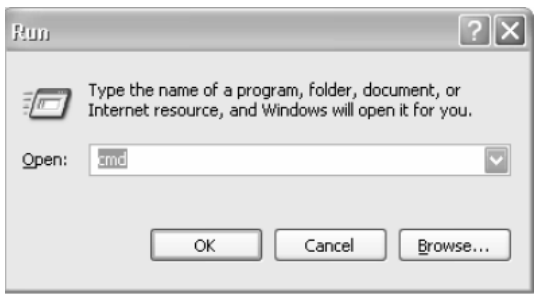


FIGURA 3.39 Ventana de comandos

Entramos en el directorio tsp-client

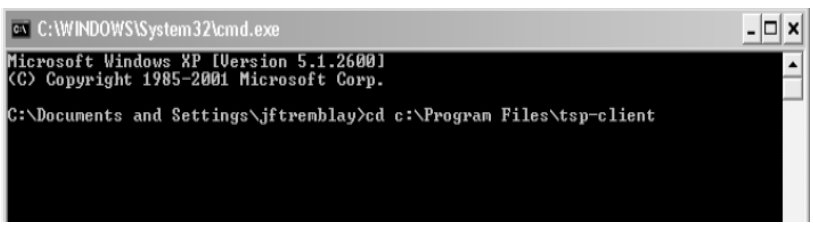


FIGURA 3.40 Cambio de Directorio a TSP-client

Al ser instalado y configurado este túnel crea uanconeccion LAN IPv6 el cual nos brinda la capacidad de conectarnos con clientes IPv6

FIGURA 3.41 Conexión de área local creada por el tunel

5.3CONFIGURACIÓN DE DOMAIN NAME SYSTEM "DNS" MEDIANTE EL PROTOCOLO IPV6

La implementación de servidores DNS se la realizo bajo sistemas operativos Microsoft utilizando los registros AAAA para identificar hosts IPv6.

Lo primero que debemos hacer es verificar que se encuentre instalado el servicio DNS en nuestro

Servidor para lo que vamos a inicio, programas, herramientas administrativas, servicios

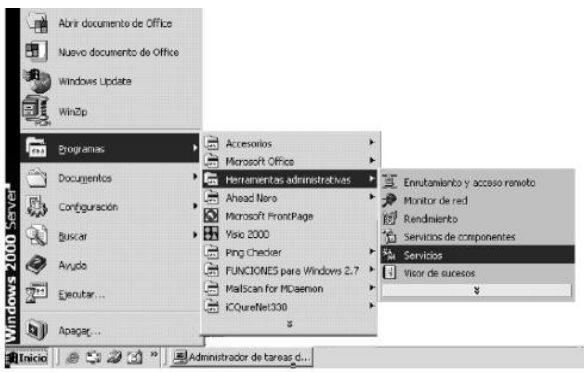


FIGURA 3.42 Verificación del DNS instalado

Una vez que nos encontramos en el detalle de servicios buscamos que se encuentre el servidor DNS, en caso de no tenerlo debemos instalar este servicio.

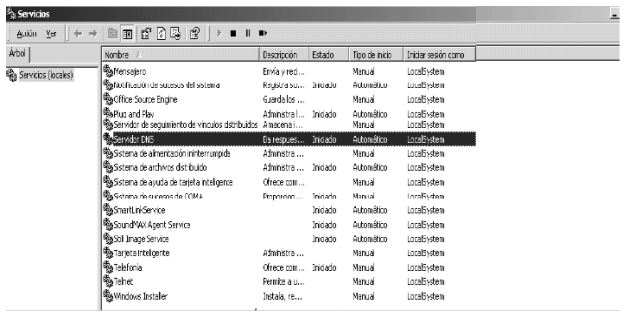


FIGURA 3.43 Verificación de instalación del servidor DNS

Cuando esta instalado el servidor DNS en mi servidor procedemos a configurar una nueva zona primaria, para esto realizamos el siguiente procedimiento:

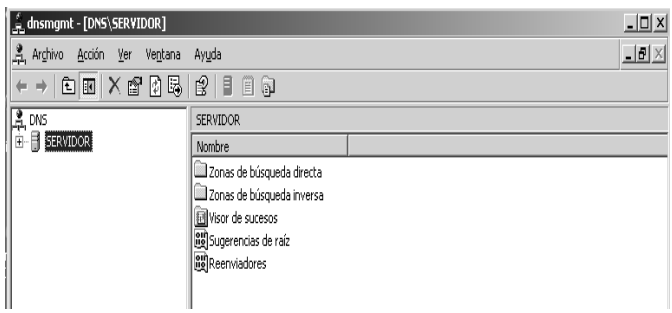


FIGURA 3.44 Creación de Zonas en DNS

En zona de búsqueda directa procedemos a crear una nueva zona que corresponde al dominio en que trabajaremos, utilizamos el asistente para crear la zona

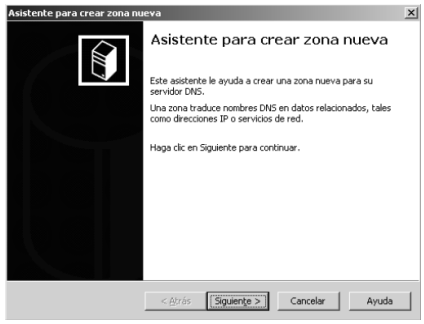


FIGURA 3.45 Inicio del asistente de creación de zonas

Ingresamos el tipo de zona

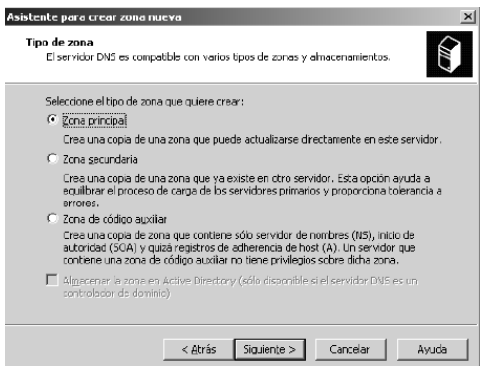


FIGURA 3.46 Elegimos Zona principal

Y el nombre de nuestro dominio, en este caso como es un laboratorio local utilizamos cualquier nombre. Secv6.espe.edu nombre del archivo donde se guardan los datos de la zona

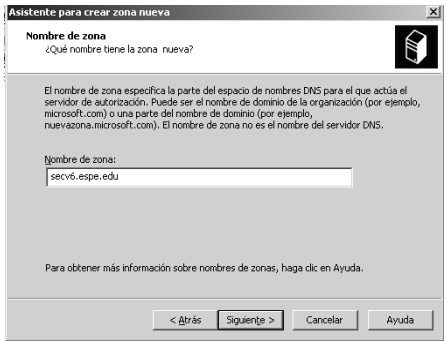


FIGURA 3.47 Ingresamos el nombre de la Zona

Una vez creada la zona finalizamos el asistente; luego creamos la zona inversa que s igual al la zona directa.

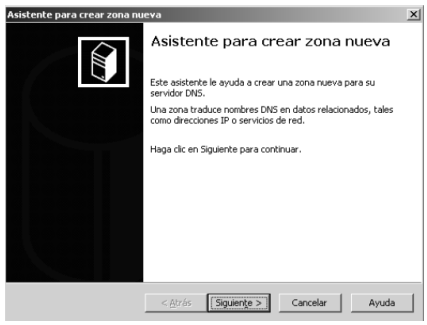


FIGURA 3.48 Inicio del asistente para crear zonas inversas

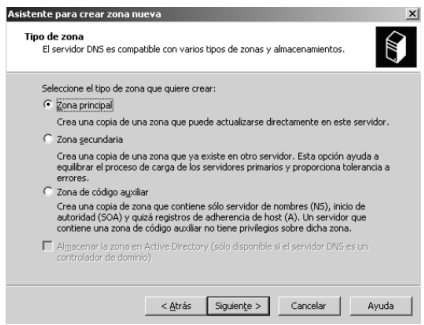


FIGURA 3.49 Seleccionamos zona principal

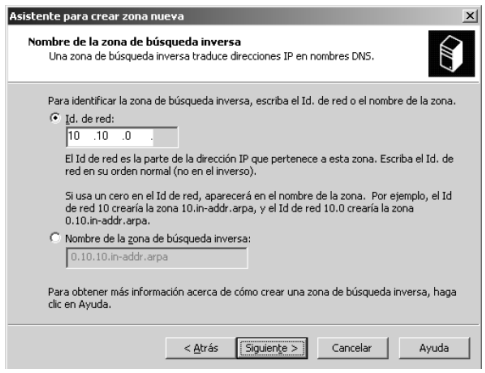


FIGURA 3.50 Dirección inversa IPv4

FIGURA 3.51 Dirección inversa

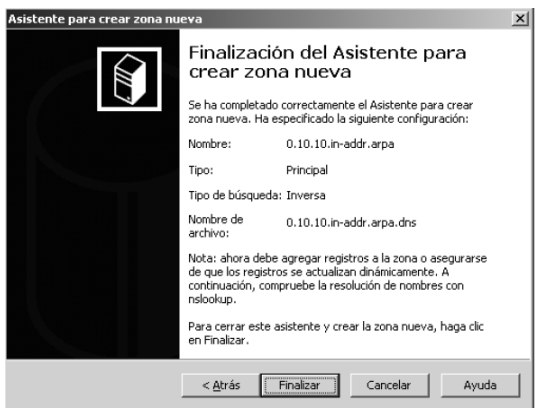


FIGURA 3.52 Fin del asistente de creación de zona

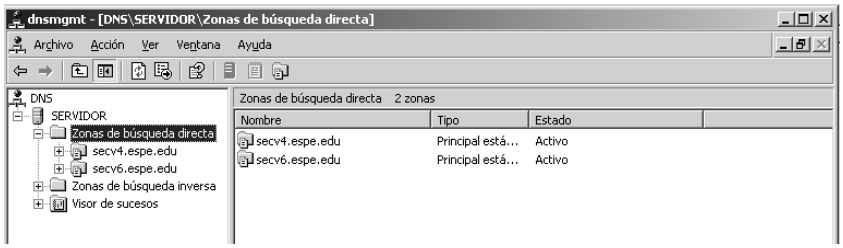


FIGURA 3.53 Zonas creadas para conexión IPv6 e IPv4

Luego procedemos a crear los host que requerimos utilizar con IPv4 e IPv6

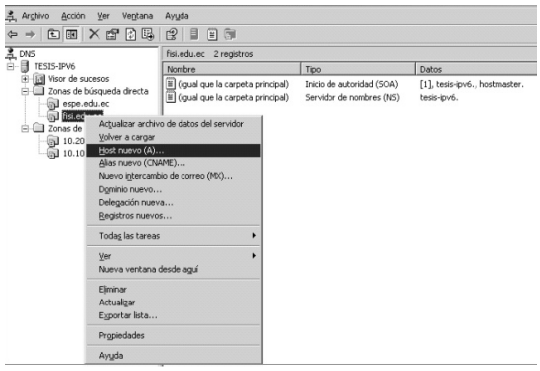


FIGURA 3.54 Creación de Registros IPv4

Para crear los clientes de nuestra red IPv6 nos dirigimos hacia Registros Nuevos

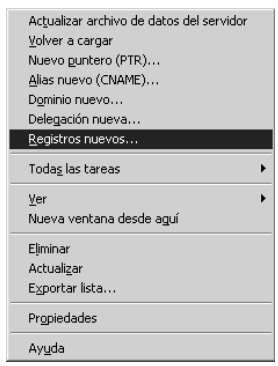


FIGURA 3.55 Escogemos Registros Nuevos para IPv6

Escogemos host IPv6 (AAAA)

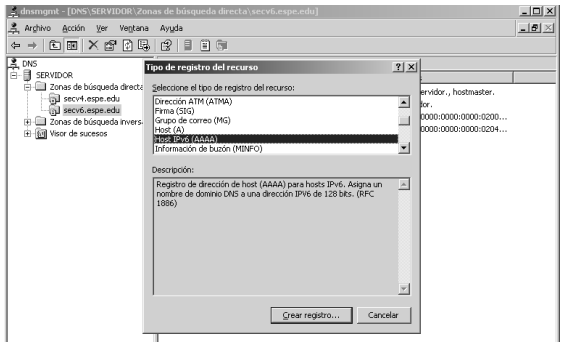


FIGURA 3.56 Escogemos el tipo de registro (AAAA)

Donde irá el nombre de nuestros clientes y la dirección IPv6

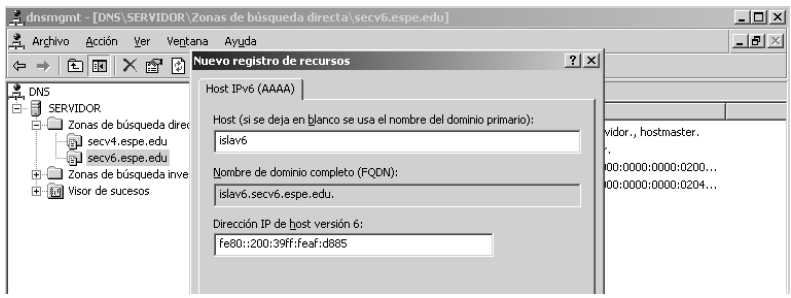


FIGURA 3.57 Creamos los clientes IPv6

5.4 PRUEBAS DE CONECTIVIDAD CON EL PROTOCOLO IPV6 ENTRE CLIENTE SERVIDOR

Para comprobar la conectividad que tenemos entre el cliente y el Servidor ejecutamos en la ventana de comandos de Cliente un ping6 con la dirección IPv6 del servidor y obtendremos respuesta de conectividad.

Al igual desde el servidor ejecutamos un ping6 con al dirección Ipv6 de este hacia el cliente y tendremos respuesta de conectividad.

5.5 CONFIGURACIÓN DE NUEVAS DIRECCIONES DE RED GLOBALES Y LOCALES Y DE SITIO

Al configurar la dirección IPv6 en clientes y servidores, se crea automáticamente la dirección local o link local, mientras que las direcciones Globales y de Sitio las podemos creadas.

Bajo el ambiente Linux el método es el siguiente:

Direcciones Globales

/sbin/ip eth0 inet6 add 3ff:ffff:0:10:2:2ª01:2/64

Direcciones de Sitio

//sbin/ip eth0 inet6 add fec0::1:250:b7:ff:fe14:35d0/64

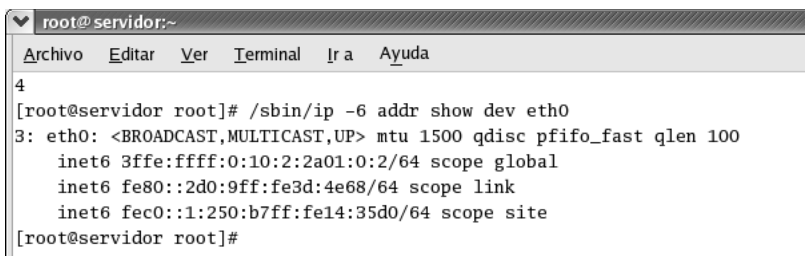


FIGURA 3.58 Direcciones Ipv6 Locales Globales y de Sitio

5.6 COMPROBACIÓN DE LAS VENTAJAS DEL PROTOCOLO IPV6 (NEIGHBOR DISCOVERY)

Para descubrir los vecinos entre clientes ejecutamos el comando **Ipv6 nc**

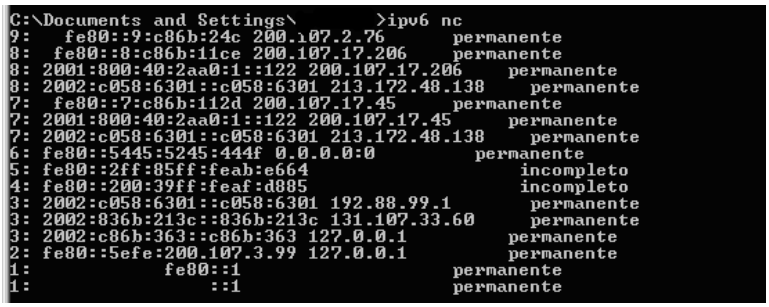


FIGURA 3.59 Descubrimiento de Vecinos bajo Internet

Encontramos varios vecinos ya que estamos conectados a Internet y dentro de un túnel broker y nos presenta vecinos que encuentran dentro de una red Ipv6 del túnel

5.7 ASIGNACIÓN DE DIRECCIÓN Y CREACIÓN DE CLIENTE IPV6 MEDIANTE INTERNET AL 6BONE

Para obtener una dirección IPv6 directamente y crear un túnel entre un cliente y el proyecto 6Bone o los servidores del proyecto debemos crear nuestro cliente vía Internet; ya que ellos nos asignan la dirección y el método para hacerlo.

IPv6 Tunnel Broker

El túnel que has solicitado ha sido configurado en nuestro extremo con éxito.
Use plan:

Debes ejecutar el siguiente fragmento de código para configurar el túnel en tu extremo.

```
netsh interface ipv6 add v6v4tunnel Consulintel 200.107.17.45 213.172.48.138
netsh interface ipv6 add address Consulintel 2001:800:40:2AA0:0001::122
netsh interface ipv6 add route 0::/0 Consulintel publish=yes
```

Si tu máquina tiene una dirección privada, necesitarás que el router del extremo cliente soporte el envío del protocolo 41.

FIGURA 3.60 Configuración del extremo del túnel

A demás que al para tener conexión con el servidor necesitamos configurar el extremo del túnel del cliente

FIGURA 3.61 Configuración del túnel en Windows XP

Una vez creado el cliente, podemos ver la dirección asignada a nuestro cliente en la dirección http://tb4.consulintel.euro6ix.org/es/autentica.php.

IPv6 Tunnel Broker

Tunnel Activo
Tunnel Inactivo

Nombre	Dirección IPv4	Dirección IPv6 del Cliente	Dirección IPv6 del Servidor	Dominio / Fecha de Baja	
tb-0088	200.107.17.45	2001:800:40:2AA0:0001::122	2001:800:40:2AA0:0001::251	tesis.tb.consulintel.euro6ix.net	Eliminar

FIGURA 3.62 Direcciones IPv6 del cliente y Sevidor

Donde podemos verificar nuestra dirección IPv6 del cliente que a sido asignada, la dirección Ipv6 del servidor al cual estamos conectados y nuestro dominio

Dir IPv6 Cliente Windows XP: 2001:800:40:2AA0:0001::122
Dir Servidor 6bone 2001:800:40:2AA0:0001::251
Dominio: tesis.tb.consulintel.euro6ix.net

Este tunnel tiene un tiempo de vida de 2 meses y se lo puede ampliar; este tiempo de vida es asignado el momento de su creación.

Para comprobar que el túnel se encuentran configurado en nuestra máquina verificamos mediante

IPv6 if

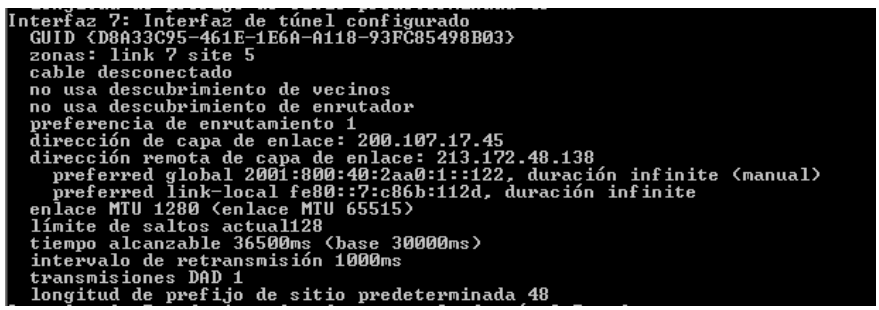


FIGURA 3.63 Comprobación de la dirección asignada

También se lo puede hacer para descubrimiento de vecinos en conexione cliente servidor

Debido a que la ESPE-L posee servidores con sistema operativo Linux y Server 2000 se presenta la configuración de cada uno de ellos, además del sistema operativo 2003 Server que en el momento de la migración se lo recomienda en reemplazo del servidores bajo 2000 Server.

Para el caso de el SERVER NT DE DOMINIO DE DESARROLLO VIRTUAL el sistema operativo a usar es Windows 2003 Server, en el SERVER LINUX la versión Linux Fedora o Debian, y en los SERVER NT DOMINIO y SERVER 2000 APLICACIONES PRODUCCION serán reemplazado por Windows 2003 Server

Además se deberá instalar el servicio de tuneling ya que los servidores mantendrán comunicación también con clientes bajo protocolo IPv4

Para los laboratorios de Internet y máquinas con salida a Internet se deberá utilizar el Sistema Operativo Windows XP y configurar túneles como hexago o consulintel para tener enlace con servidores IPv6 y pertenecer a una isla IPv6.

CAPITULO IV

CONCLUSIONES Y RECOMNENDACIONES

CONCLUSIONES

Como conclusiones se puede decir

- Al realizar encuestas y entrevistas, se obtuvo como resultado que el personal del área de sistemas e informática y alumnos no conocían sobre el protocolo por lo que luego se procedió a realizar una explicación básica sobre el protocolo IPv6.

- Al ser proyecto investigativo y de última tecnología se necesito de cierto grado de esfuerzo empleado en la búsqueda de información en la Internet lo cual llevó más tiempo de lo previsto.

- Actualmente los proveedores de servicio de Internet ISP´s no poseen mucha información del protocolo IPv6 así como tampoco tienen proyectos para brindar conexión a través de IPv6, por lo que no se pudo obtener información sobre el protocolo en sí o de algún proyecto a futuro.

- La utilización de Software con IPv6 preinstalado evitará muchos inconvenientes como tiempo, caso contrario se deberá bajar parches de la Internet lo que llevará mucho tiempo debido al tamaño del archivo y al momento de la instalación.

- Al instalar los parches tener en cuenta que archivos se tiene que configurar y activar para uso del protocolo IPv6 y cuales no necesitan de activación.

- Establecer una metodología y desarrollarla paso a paso para que el momento de migrar no se tenga conflictos, daños y pérdida de tiempo en la puesta en macha a la red.

- Al ser una metodología desarrollada para las redes de la ESPE-L, la configuración se debería desarrollar en los servidores de la misma, pero tomando en cuenta la importancia de los servicios que presta cada unos de los servidores y del tiempo que llevaría desarrollar el proyecto se tomo como alternativa desarrollar un prototipo de la intranet de la ESPE-L la misma que fue instalada configurada y puesta en funcionamiento bajo el protocolo IPv6 obteniéndolos satisfactoriamente resultados deseados.

  De igual manera se hizo la conexión a Internet, tomando un servidor que se encuentre configurado el protocolo IPv6 y el túnel hexago, dicho servidor tenía enlace con el servidor Ipv6 del Consulintel.

4.2 RECOMENDACIONES

Como recomendaciones se puede decir

- Investigar el grado de conocimiento sobre el protocolo IPv6 dentro del área de Sistemas e Informática antes de iniciar un proyecto de migración; y de acuerdo a al resultado iniciar una capacitación sobre configuración del mismo.

- Utilizar software de última tecnología como Windows 2003 Server y Windows XP, ya que vienen con el protocolo IPv6 preinstalado y no necesita de parches.

- Utilizar Linux Gentoo, Debian o Fedora en versiones 8.0 en adelante ya que vienen con el modulo IPv6 ya cargado, además de tener herramientas que facilitan el uso del protocolo IPv6.

- Incrementar la difusión y formación de IPv6 en la comunidad académica y a mismo tiempo incentivar a desarrollar proyectos con IPv6

ANEXO 2.1

ENCUESTA

El siguiente cuestionario permitirá saber acerca de los conocimientos básicos que usted posee de los protocolos ipv4 e ipv6 y cuales son las expectativas que usted tiene ante lo la tecnología que nos brinda la espe-l a los docentes y estudiantes.

Estudiante ( ) Administrativo ( ) Profesor ( )

1.- ¿ conoce usted que tipo de dirección de red (clase a,b, o c) y cual es el tamaño de la dirección que se utiliza en la espe-l ?

si ( ) no ( )

2.- ¿ conoce los protocolos de enrutamiento que utiliza el protocolo ipv4 ?

Si ( ) no ( )

3.- ¿ a escuchado de las desventajas que presenta el protocolo ipv4 ?

Si ( ) no ( )

4.- ¿ a escuchado sobre en nuevo protocolo ipv6 y las ventajas que nos presentaría este al utilizarlo?

Si ( ) no ( )

5.- ¿ sabía que el tamaño de dirección del protocolo ipv6 es de 8 bits ?

Si ( ) no ( )

6.- ¿ sabía que el nuevo protocolo ipv6 tiene diferente forma de enrutamiento de los paquetes que el protocolo ipv4 ?

Si ( ) no ( )

7.-¿ conoce o a escuchado sobre alguna técnica de migración de redes ipv4 a redes ipv6?

Si ( ) no ( )

8.- ¿ de las técnicas de migración, sabe usted cual es la más utilizada o recomendada ?

Si ( ) no ( )

9.- ¿ desearía que la espe -l empleará este el nuevo protocolo ?

Si ( ) no ( )
porqué……..……..……

ANEXO 2.2

ENTREVISTAS

NOMBRE:

1.- A TENIDO ALGÚN PROBLEMA CON LOS SERVICIOS O AL UTILIZAR EL PROTOCOLO IPV4

……
……
……
……

2.- SABE USTED EL TAMAÑO Y VENTAJAS QUE NOS BRINDA EL PROTOCOLO IPV6

……
……
……
……
……

3.- CONOCE ALGUNA TÉCNICA DE MIGRACIÓN O SABE CUAL DE ESTAS SE A EMPLEADO EN ALGUNA INSTITUCIÓN

……
……
……
……

4.- CREE QUE SE DEBERÍA IMPLANTAR IPV6 Y QUE BENEFICIOS CREE QUE TRAERÁ LA IMPLANTACIÓN ESTE PROTOCOLO EN LA RED DE LA ESPE-L

……
……
……
……
……

5.- CONSIDERA NECESARIO LA MIGRACIÓN AL NUEVO PROTOCOLO IPV6 Y POR QUE

……
……
……
……
……

6.- PIENSA QUE TODOS LOS SERVICIOS QUE NOS BRINDA EL NUEVO PROTOCOLO AYUDARÁ A LAS REDES, ESTUDIANTES O SERVICIOS QUE OFRECE LA ESPE-L

……
……
……

ANEXO 3.1

COMANDOS BASICOS DE IPV6 BAJO LINUX

Mostrar direcciones ipv6

Se puede hacer mediante el uso de **ip** o **ifconfig**:

#> /sbin/ip -6 addr show dev <interface>

#> /sbin/ifconfig <interface>

Añadir una dirección ipv6

Se puede hacer mediante el uso de **ip** o **ifconfig**:

#> /sbin/ip -6 addr add <ipv6address>/<prefixlength> dev <interface>

#> /sbin/ifconfig <interface> inet6 add <ipv6address>/<prefixlength>

Eliminar una dirección ipv6

Se puede hacer mediante el uso de **ip** o **ifconfig**:

#> /sbin/ip -6 addr del <ipv6address>/<prefixlength> dev <interface>

#> /sbin/ifconfig <interface> inet6 del <ipv6address>/<prefixlength>

Mostrar rutas ipv6

Se puede hacer mediante el uso de **ip** o **route**:

#> /sbin/ip -6 route show [dev <device>]

#> /sbin/route -a inet6

Añadir una ruta ipv6 a través de un gateway

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route add <ipv6network>/<prefixlength> via <ipv6address>
[dev <device>]

#> /sbin/route -a inet6 add <ipv6network>/<prefixlength> gw <ipv6address>
[dev <device>]

Eliminar una ruta ipv6 a través de un gateway

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route del <ipv6network>/<prefixlength> via <ipv6address> [dev <device>]

#> /sbin/route -a inet6 del <ipv6network>/<prefixlength> gw <ipv6address> [dev <device>]

Añadir una ruta ipv6 a través de una interfaz

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route add <ipv6network>/<prefixlength> dev <device> metric 1

#> /sbin/route -a inet6 add <network>/<prefixlength> dev <device>

Eliminar una ruta ipv6 a través de una interfaz

Se puede hacer mediante el uso de ip o route:

#> /sbin/ip -6 route del <ipv6network>/<prefixlength> dev <device> metric 1

#> /sbin/route -a inet6 del <network>/<prefixlength> dev <device>

Ping6

Normalmente incluido en el paquete iputils. Uso:

#> ping6 <hostwithipv6address>

#> ping6 <ipv6address>

#> ping6 [-i <device>] <link-local-ipv6address>

Traceroute6

Normalmente incluido en el paquete iputils. Uso:

#>traceroute6

Tracepath6

Normalmente incluido en el paquete iputils. Uso:

#>tracepath6

ANEXO 3.2

COMANDOS BASICOS DE IPV6 BAJO WINDOWS

- **Ipv6 install**

  Instala el protocolo ipv6 como protocolo de red para conexiones lan.

  Ipv6 uninstall

  Quita el protocolo ipv6 como protocolo de red para conexiones lan.

- **Ipv6** [**-v**] **if** [*índicedeinterfaz*]

  Muestra información acerca de las interfaces.

- **Ipv6 ifcr v6v4** *origenv4 destinov4* [**nd**] [**pmld**]

  Crea una interfaz configurada de túnel ipv6 sobre ipv4 con las direcciones ipv4 de origen y destino especificadas.

- **Ipv6 ifcr 6over4** *origenv4*

  Crea una interfaz para 6over4 con la dirección ipv4 de origen especificada. Para obtener más información acerca de 6over4, consulte el documento rfc 2529.

- **Ipv6 ifc** *índicedeinterfaz* {[**forwards**] | [**-forwards**]} {[**advertises**] | [**-advertises**]} [**mtu** *númerodebytes*] [**site** *identificadordesitio*]

  Controla los atributos de la interfaz.

- **Ipv6 ifd** *índicedeinterfaz*

  Elimina una interfaz. Las pseudointerfaces de bucle de retroceso y de túnel automático no se pueden eliminar.

- **Ipv6 adu** *índicedeinterfaz***/***dirección* [**life** *duraciónválida*[**/***duraciónpreferida*]] [**anycast**] [**unicast**]

Agrega o quita la asignación de una dirección de unidifusión o de difusión por proximidad en una interfaz, con el valor predeterminado de unidifusión a menos que se especifique difusión por proximidad.

- **Ipv6 nc** [*índicedeinterfaz* [*dirección*]]

  Muestra el contenido de la caché de vecinos.

- **Ipv6 ncf** [*índicedeinterfaz* [*dirección*]]

  Quita las entradas especificadas de la caché de vecinos.

- **Ipv6 rc** [*índicedeinterfaz* [*dirección*]]

  Muestra el contenido de la caché de enrutamiento.

- **Ipv6** [**-v**] **rt**

  Muestra el contenido actual de la tabla de enrutamiento.

- **Ipv6 rtu** *prefijo índicedeinterfaz*[***I****dirección*]]

  Agrega o quita una ruta en la tabla de enrutamiento.

- **Ipv6 spt**

  Muestra el contenido de la tabla de prefijos del sitio.

- **Ipv6 spu** *prefijo índicedeinterfaz* [**life** *l*]

  Agrega, quita o actualiza un prefijo en la tabla de prefijos del sitio.

- **Ipv6 gp**

  Muestra los valores de los parámetros globales del protocolo ipv6.

- **Ipv6** [**-p**] **gpu defaultcurhoplimit** *saltos*

Establece el valor del campo límite de saltos del encabezado ipv6 en los paquetes enviados por el nodo.

- **Ipv6** [**-p**] **gpu useanonymousaddresses** [**yes**|**no**|**always**|*contador*]

  Determina si se utilizan o no direcciones anónimas. El valor predeterminado es **yes**. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu maxanondadattempts** *número*

  Establece el número de veces que se comprueba si una dirección anónima es única. El número predeterminado de intentos es 5. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu maxanonlifetime** *válida*[*/preferida*]

  Establece la duración válida y la duración preferida de las direcciones anónimas. La duración válida predeterminada es de 7 días. La duración preferida predeterminada es de 1 día. La opción **-p** guarda las opciones en el registro.

- **Ipv6** [**-p**] **gpu anonregeneratetime** *tiempo*

  Establece el período de tiempo (en segundos) en el que se debe generar una nueva dirección anónima. El valor predeterminado es de 5 segundos. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu maxanonrandomtime** *tiempo*

  Establece la cantidad de tiempo en minutos del tiempo aleatorio anónimo máximo. El tiempo aleatorio anónimo es el periodo de tiempo que transcurre hasta que caduca el periodo de tiempo válido en el que una dirección anónima puede generar una nueva dirección anónima. El protocolo ipv6 de windows xp elige aleatoriamente un tiempo aleatorio anónimo entre los

valores de anonrandomtime y maxanonrandomtime. El escalonado aleatorio de la regeneración de direcciones anónimas se realiza para evitar repercusiones negativas en el tráfico de red cuando muchas direcciones anónimas dejan de ser válidas simultáneamente. El valor predeterminado es de 10 minutos. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu anonrandomtime** *tiempo*

  Establece el tiempo aleatorio anónimo mínimo en segundos. El valor predeterminado es de 0 segundos. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu neighborcachelimit** *número*

  Establece el número máximo de entradas de la caché de vecinos para cada interfaz. El valor predeterminado es de 8 entradas. La opción **-p** guarda el valor en el registro.

- **Ipv6** [**-p**] **gpu routecachelimit** *número*

  Establece el número máximo de entradas de la caché de enrutamiento para cada interfaz. El valor predeterminado es de 32 entradas. La opción **-p** guarda el valor en el registro.

- **Ipv6 ppt**

  Muestra la tabla de directivas de prefijos. La tabla de directivas de prefijos se utiliza para especificar las directivas de selección de direcciones de origen y destino.

- **IPV6 PPU** *PREFIJO* **PRECEDENCE** *VALORDEPRIORIDAD* **SRCLABEL** *valordeetiquetadeorigen* [**dstlabel** *valordeetiquetadedestino*]

  Actualiza la tabla de directivas de prefijos con una directiva que especifica la prioridad, un valor de etiqueta de origen (*valordeetiquetadeorigen*) y un valor

de etiqueta de destino (*valordeetiquetadedestino*). Las entradas de la tabla de directivas de prefijos pueden modificar el comportamiento de la selección de direcciones de origen y destino. Para obtener más información, consulte el borrador de internet titulado "default address selection for ipv6" (selección de direcciones predeterminadas en ipv6).

- **IPV6 RENEW** [*ÍNDICEDEINTERFAZ*]

Renueva la configuración de ipv6 en todas las interfaces. Si se especifica un número de índice de interfaz, sólo se renovará la configuración de esa interfaz. Para un host, las direcciones configuradas automáticamente se actualizan enviando mensajes de solicitud de enrutador en las interfaces correspondientes. Las direcciones se vuelven a configurar en función de los mensajes de anuncio de enrutador recibidos

Latacunga, 12 de abril de 2005

WENDY VASQUEZ ARMENDARIZ
AUTOR

Ing. Santiago Jácome Guerrero
DECANO DE LA FACULTAD DE SISTEMAS E INFORMÁTICA

Dr. Eduardo Vázquez Alcázar
SECRETARIO ACADEMICO ESPE-L