



UNIVERSIDAD AUTONOMA DEL ESTADO DE MEXICO
CENTRO UNIVERSITARIO UAEM TEXCOCO

“CREACIÓN DE UNA RED HIBRIDA EN IPV6 QUE COEXISTA CON UNA RED IPV 4 EN
CRUZ ROJA MEXICANA I.A.P. DELEGACION DISTRITO FEDERAL”

T E S I S

QUE PARA OBTENER EL TITULO DE
LICENCIADO EN INFORMATICA ADMINISTRATIVA

P R E S E N T A:

CARAVES MUÑOZ ENRIQUE
MARCIAL LOPEZ NESTOR ADRIAN

DIRECTOR:

ING. JOSE ROBERTO RAMIREZ CERVANTES

REVISORES:

M. EN C. A. LETICIA ARÉVALO CEDILLO
M. EN C. FÉLIX RAMÍREZ CERVANTES

Texcoco, México. Febrero 2014

Texcoco, Mex. A 11 de Diciembre De 2013

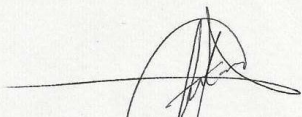
M. en C. JUAN MANUEL MUÑOZ ARAUJO
SUBDIRECTOR ACADEMICO DEL
CENTRO UNIVERSITARIO UAEM TEXCOCO
PRESENTE

COPIA

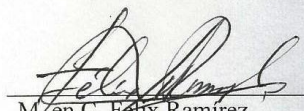
AT'N EN P.P ANTONIO INOUE CERVANTES
RESPONSABLE DEL DEPARTAMENTO DE TITULACION

Con base en la revisiones efectuadas al trabajo escrito titulado **“Creación de una red hibrida en IPv6 que coexista con una red IPv 4 en cruz roja mexicana I.A.P. delegación distrito federal”** que para obtener el título de **Licenciado en Informática Administrativa** presenta el sustentante **C. ENRIQUE CARAVES MUÑOZ**, con número de cuenta **0014223** respectivamente, se concluye que cumple con los requisitos teórico-metodológicos por lo que se le otorga el voto aprobatorio para sustentación, pudiendo **continuar con la etapa de digitalización** del trabajo escrito.


ATENTAMENTE

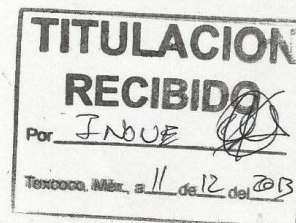

M. en C. Leticia Arevalo
Cedillo

REVISOR


M. en C. Felix Ramirez
Cervantes

REVISOR


Ing. José Roberto Ramírez Cervantes
DIRECTOR



Texcoco, Mex. A 11 de Diciembre De 2013


M. en C. JUAN MANUEL MUÑOZ ARAUJO
SUBDIRECTOR ACADEMICO DEL
CENTRO UNIVERSITARIO UAEM TEXCOCO
PRESENTE

COPIA

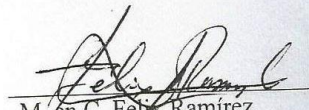
AT'N EN P.P ANTONIO INOUE CERVANTES
RESPONSABLE DEL DEPARTAMENTO DE TITULACION

Con base en la revisiones efectuadas al trabajo escrito titulado **“Creación de una red hibrida en IPv6 que coexista con una red IPv 4 en cruz roja mexicana I.A.P. delegación Distrito Federal”** que para obtener el título de **Licenciado en Informática Administrativa** presenta el sustentante **C. NESTOR ADRIAN MARCIAL LOPEZ**, con número de cuenta **0422352** respectivamente, se concluye que cumple con los requisitos teórico-metodológicos por lo que se le otorga el voto aprobatorio para sustentación, pudiendo **continuar con la etapa de digitalización** del trabajo escrito.

ATENTAMENTE


M. en C. Yencia Arevalo
Cedillo

REVISOR


M. en C. Felix Ramirez
Cervantes

REVISOR


Ing. José Roberto Ramírez Cervantes
DIRECTOR



Agradecimientos

A la U.A.E.M.

Por darme los conocimientos, habilidades y valores necesarios para llevar a buen término este proyecto.

A la CRUZ ROJA MEXICANA I.A.P. DELEGACIÓN DISTRITO FEDERAL

Por apoyarnos en nuestro desarrollo como profesionistas y permitirnos todas las facilidades en el desarrollo del proyecto.

Al ING. JOSÉ ROBERTO RAMÍREZ CERVANTES

Por su guía y paciencia en el desarrollo del presente. Mas por su gran dedicación y ejemplo durante su dirección.

A la M. EN C. A. LETICIA ARÉVALO CEDILLO y el M. EN C. FÉLIX RAMÍREZ CERVANTES

Por hacernos mejores, mostrándonos nuestras debilidades y potenciando nuestras aptitudes.

Dedicatorias

Para Enrique Caravez Juárez y María del Consuelo Muñoz Magaña.

Les dedico este pequeño triunfo y aprovecho para darles las gracias por su apoyo incondicional y sincero a lo largo de toda mi vida, por inculcarme los valores y virtudes que me han hecho llegar en donde estoy el día de hoy.

Para María del Consuelo Caraves Muñoz y Antonio Basilio Yáñez.

Gracias por haberme apoyado siempre en mi carrera profesional y por compartir tantas experiencias y buenos momentos conmigo.

Para Ernesto Caraves Muñoz y Marisela Pinos García.

Gracias por ser un ejemplo a seguir, por ayudarme a dar este pasó en mi carrera profesional y por siempre estar ahí.

Para Alejandra Caraves, Andrea Caraves, Marco Polo Caraves y Dana Fernanda Caraves.

Algunos de ustedes van más avanzados en su vida que otros y cada uno en su momento me apoyado en su manera, gracias por todo.

Para Anabel Paredes López

Gracias por todo, sin ti nada de esto sería posible, ahora somos 2 contra el mundo.

Para Adrian Marcial Villegas y Ángela López García

Porque ustedes han sido un gran ejemplo en mi vida y si el día de hoy puedo decir que si he podido ser alguien es por ustedes.

Gracias por su apoyo.

Para Yoloth Osiris Marcial Amaro y Michel Alexander Marcial Amaro

Yo sé que ustedes no pueden leer esto en estos momentos, pero cuando puedan, les voy pedir que cada uno me tiene que entregar su propia tesis cuando sea su momento.

Para Cristihan Alexandra Gonzalez Lira.

Por ser el motor en mí día a día, mí musa, mi sol. Quiero estar de la mano siempre contigo.

Índice

Introducción	12
Planteamiento del problema	13
Justificación	14
Objetivo general.....	15
Objetivos particulares	15
Hipótesis.....	16
Capítulo 1 Definición de Redes Informáticas.	17
1.1 Generalidades de las redes.....	17
1.2 Componentes básicos de las redes.....	17
1.3 ¿Qué es una red informática?	18
1.4 Tipos de redes.....	19
1.4.1 Redes Por Alcance.	19
1.4.2 Redes Por Tipo De Conexión.....	20
1.4.3 Redes Por Relación Funcional.....	20
1.4.4 Redes Por Topología.....	21
1.4.5 Redes Por Direccionalidad De Datos.	21
1.4.6 Redes Según Grado De Autenticación.....	22
1.4.7 Según Grado De Difusión.	22
1.4.8 Redes Según Servicio o Función.	22
1.5 Importancia de las redes en la actualidad.....	23
1.6 Ventajas de las redes informáticas:	23
Capítulo 2 Concepto e Historia de IPV6.....	24
2.1 Concepto de IPV6.....	24
2.2 ¿Por qué surge?.....	24
2.3 Situación actual.....	24
2.4 Historia de IPV6	25
2.5 IPV6 en México.....	25
2.6 Características principales	27
2.7 ¿Qué tan grande es el espacio de direcciones?	28
2.7.1 Direccionamiento	28
2.8 DNS	31
2.9 Mecanismos de transición básicos	31

2.9.1 Dual Stack	32
2.9.2 Tunneling	32
Capítulo 3 Análisis y Diseño de la Red.....	33
3.1 Diseño de la red	33
3.2 Características a considerar de la red	33
3.3 Descripción de la nueva red.	34
3.3.1 Cobertura de la red	34
3.3.2 Necesidades	34
3.3.3 Topología	35
3.3.4 Metodología	35
3.3.4.1 Conexión a Internet IPv4.....	36
Capítulo 4 Concepto de virtualización y pruebas.	38
4.1 Virtualización de la red.	38
4.1.1 Generalidades de la virtualización	39
4.1.2 Definición de virtualización.....	40
4.1.3 Tipos de virtualización.....	41
4.1.4 Las razones de virtualizar.	42
4.1.5 Herramienta de virtualización a utilizar.....	44
4.1.6 instalación de VMware Workstation 10.0.....	44
4.1.7 Creación de una máquina virtual.....	45
4.1.8 Instalación de sistema operativo en una máquina virtual	50
4.1.9 Ejecución de la máquina virtual.....	52
4.1.10 Instalación de Ipv6 en Windows XP	54
4.2 Configuración del router	54
4.2.1 Configuración de router cisco para 6to4.....	55
4.2.2 Configuración de 6pe.....	55
4.2.3 Configuración de nat 64	56
4.2.4 Implementación de un dns64	57
4.3 Pruebas virtualizadas	58
4.3.1 Prueba 6to4	59
4.3.2 Prueba Nat64.....	59
4.3.3 Prueba de cliente servidor	60
4.4 Implementación física.....	60

4.4.1. Pruebas físicas	61
4.4.2 Prueba 6to4 (física).....	61
4.4.3 Prueba Nat64 (física).....	62
4.4.4 Prueba de cliente servidor	63
Conclusiones	64
Bibliografía.....	65

Índice de Figuras

Figura 1	Redes Informaticas.....	18
Figura 2	Redes por Alcance.....	19
Figura 3	Redes por su conexión.....	20
Figura 4	Redes con servidores.....	20
Figura 5	Topologías de red.....	21
Figura 6	Redes por modo de transmisión.....	21
Figura 7	Internet-Intranet.....	22
Figura 8	Longitud del prefijo Ejemplo 1.....	30
Figura 9	Longitud del prefijo Ejemplo 2.....	30
Figura 10	Longitud del prefijo Ejemplo 3.....	30
Figura 11	Tunneling.....	32
Figura 12	Captura 1.....	45
Figura 13	Captura 2.....	46
Figura 14	Captura 3.....	46
Figura 15	Captura 4.....	47
Figura 16	Captura 5.....	47
Figura 17	Captura 6.....	48
Figura 18	Captura 7.....	48
Figura 19	Captura 8.....	49
Figura 20	Captura 9.....	49
Figura 21	Captura 10.....	50
Figura 22	Captura 11.....	51
Figura 23	Captura 12.....	52

Índice de Tablas

Tabla 1	Tipos de Virtualización y Características.....	41
Tabla 2	Prueba 6to4 1.....	55
Tabla 3	Prueba 6to4 2.....	59
Tabla 4	Prueba 6to4 3.....	60
Tabla 5	Prueba 6to4 4.....	61
Tabla 6	Prueba 6to4 5.....	62

Introducción

Las redes informáticas son indispensables en el flujo de información diario de una institución, ya que de ellas depende la correcta comunicación, almacenamiento y ejecución de los datos en el día a día que permite llevar a cabo los procesos y trabajos adecuados en tiempo y forma.

Una red informática o de computadoras es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

El crecimiento de las redes informáticas de manera vertiginosa dificulta la administración de direcciones IP, siendo esto uno de los problemas a los que se enfrentan los administradores de redes día a día, ya que el crecimiento de las redes hace que las direcciones IP escaseen en una red.

Esta misma circunstancia se plantea en la “CRUZ ROJA MEXICANA I.A.P. DELEGACION DISTRITO FEDERAL” debido a que ahora con el surgimiento del expediente clínico electrónico, establecido con la norma NOM-024-SSA3-2010, se necesitan incorporar a la red más equipos, pero el crecimiento gradual de la red, la utilización de IP versión 4 y la necesidad de otro segmento están dejando sin direcciones IP a la red.

Por ello se pretende con el siguiente trabajo establecer la instalación de un segmento más de red pero utilizando IP versión 6, para que el crecimiento de la red no afecte el correcto funcionamiento de la misma exponiendo las ventajas de la utilización de IP versión 6.

Planteamiento del problema

Actualmente la cruz roja mexicana se encuentra con pocas direcciones IP ya que utiliza IP's estáticas y utilizan la versión 4, lo cual limita mucho el crecimiento de la misma red.

Ahora con la instauración de la norma NOM-024-SSA3-2010 que marca que debe existir un expediente electrónico, lo cual requiere al menos para la institución la cantidad de 20 equipos, es decir 20 direcciones lo cual compromete el número de direcciones IP disponibles, con posibilidad de agregar más equipos en un futuro, requiriendo más direcciones para su integración a la red.

Por otro lado el crecimiento habitual de la red institucional compromete demasiado la disponibilidad de IP's, ya que debido a la creación de nuevas tecnologías, la institución se va actualizando y agregando nuevos dispositivos que requieren su integración a la red, como impresoras vía IP, tomógrafos, reloj checador de huella digital, etc.

Justificación

Anteriormente la Cruz Roja operaba el expediente de manera física lo cual dificultaba el manejo, la distribución y el compartir datos de dichos expedientes.

El manejo puesto que para archivar los datos del expediente se necesitaban espacios muy grandes y específicos lo cual restaba espacio en la institución el cual podría aprovechar para una mejor atención de los usuarios.

En distribución nos referimos de manera interna de la institución, existe poca disponibilidad e ineficientes mecanismos de búsqueda y control de datos. Lo cual limita la eficiencia en el trabajo de otras áreas por la desinformación del paciente.

En cuestión de distribución no existen mecanismos para distribuir datos o compartirlos con otra institución similar, lo cual limitaba en gran medida la recepción y el envío de expedientes.

Debido a la norma NOM-024-SSA3-2010 la institución Cruz Roja Mexicana Delegación Distrito Federal tiene la necesidad de implementar en sus instalaciones una serie de equipos que permitan la creación y almacenamiento del expediente electrónico que establece dicha norma.

Pero debido a que la red con la cuenta actualmente la institución está administrada con direcciones IP fijas y casi todas estas ya han sido asignadas, se necesitan más direcciones y de la misma forma prever para el crecimiento de dicho proyecto puesto que la tendencia cada año en la institución es de mayor demanda de beneficiarios

El impacto que se busca para la institución no solo es el manejo de expediente electrónico sino también que este sea un recurso que permita certificar bajos los estándares de las instituciones evaluadoras de calidad.

Objetivo general

Diseñar y Crear una red informática en “CRUZ ROJA MEXICANA IAP DELEGACION DISTRITO FEDERAL” que coexista con la de la institución pero utilizando el protocolo IP versión 6 solucionando el crecimiento de red en dicho lugar.

Objetivos particulares

Primer Objetivo particular

Diseñar la red de IP versión 6 que pueda coexistir con la de IP versión 4 de la institución, que a su vez no genere ningún conflicto y más aun de un mayor beneficio.

Segundo Objetivo particular

Instalar la red IP versión 6 de manera funcional y efectiva para la institución con los beneficios de uso de este nuevo protocolo.

Hipótesis

Con la creación de esta nueva subred se cubrirá el nuevo proyecto de “CRUZ ROJA MEXICANA IAP DELEGACION DISTRITO FEDERAL” Expediente Electrónico y facilitará el acceso a datos de los pacientes de manera eficiente, la red no colapsará por falta de IP's, ni limitará el trabajo por falta de las mismas.

Capítulo 1 Definición de Redes Informáticas.

1.1 Generalidades de las redes.

El primer indicio de redes de comunicación fue de tecnología telefónica y telegráfica. En 1940 se transmitieron datos desde la Universidad de Darmouth, en Nuevo Hampshire, a Nueva York. A finales de la década de 1960 y en los posteriores 70 fueron creadas las minicomputadoras. En 1976, Apple introduce el Apple I, uno de los primeros ordenadores personales. En 1981, IBM introduce su primera PC. A mitad de la década de 1980 las PC comienzan a usar los módems para compartir archivos con otras computadoras, en un rango de velocidades que comenzó en 1200 bps y llegó a los 56 kbps (comunicación punto a punto o *dial-up*).

1.2 Componentes básicos de las redes.

Para poder formar una red se requieren elementos: hardware, software y protocolos. Los elementos físicos se clasifican en dos grandes grupos: dispositivos de usuario final (*hosts*) y dispositivos de red. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

El fin de una red es la de interconectar los componentes hardware de una red, y por tanto, principalmente, las computadoras individuales, también denominados *hosts*, a los equipos que ponen los servicios en la red, los servidores, utilizando el cableado o tecnología inalámbrica soportada por la electrónica de red y unidos por cableado o radiofrecuencia. En todos los casos la tarjeta de red se puede considerar el elemento primordial, sea ésta parte de un ordenador, de un conmutador, de una impresora, etc. y sea de la tecnología que sea (Ethernet, Wi-Fi, Bluetooth, etc.)

1.3 ¿Qué es una red informática?

Es un conjunto de equipos informáticos y software conectados entre sí por medio de dispositivos físicos y/o lógicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos, con la finalidad de compartir información, recursos y ofrecer servicios.

Como en todo proceso de comunicación se requiere de un emisor, un mensaje, un medio y un receptor. La finalidad principal para la creación de una red de computadoras es compartir los recursos y la información en la distancia, asegurar la confiabilidad y la disponibilidad de la información, aumentar la velocidad de transmisión de los datos y reducir el costo general de estas acciones. Un ejemplo es Internet, la cual es una gran red de millones de computadoras ubicadas en distintos puntos del planeta interconectadas básicamente para compartir información y recursos.

La estructura y el modo de funcionamiento de las redes informáticas actuales están definidos en varios estándares, siendo el más importante y extendido de todos ellos el modelo TCP/IP basado en el modelo de referencia OSI. Este último, estructura cada red en siete capas con funciones concretas pero relacionadas entre sí; en TCP/IP se reducen a cuatro capas. Existen multitud de protocolos repartidos por cada capa, los cuales también están regidos por sus respectivos estándares.

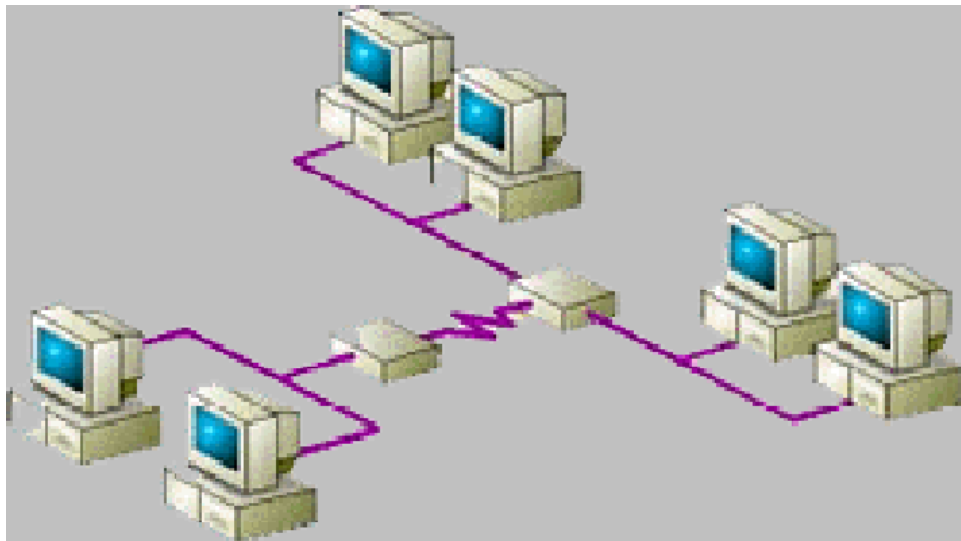


Figura 1

1.4 Tipos de redes.

La utilidad de la Red es compartir información y recursos a distancia, procurar que dicha información sea segura, esté siempre disponible, y por supuesto, de forma cada vez más rápida y económica.

Una red informática tiene distintos tipos de clasificación dependiendo de su estructura o forma de transmisión, entre los principales tipos de redes están los siguientes:

- Redes por Alcance
- Redes por tipo de conexión
- Redes por relación funcional
- Redes por Topología
- Redes por Direccionalidad
- Redes por grado de autenticación
- Redes por grado de difusión
- Redes por servicio y función

1.4.1 Redes Por Alcance.

Este tipo de red se nombra con siglas según su área de cobertura: una red de área personal o PAN (Personal Área Network) es usada para la comunicación entre dispositivos cerca de una persona; una LAN (Local Área Network), corresponde a una red de área local que cubre una zona pequeña con varios usuarios, como un edificio u oficina. Para un campus o base militar, se utiliza el término CAN (Campus Área Network). Cuando una red de alta velocidad cubre un área geográfica extensa, hablamos de MAN (Metropolitan Área Network) o WAN (Wide Área Network). En el caso de una red de área local o LAN, donde la distribución de los datos se realiza de forma virtual y no por la simple direccionalidad del cableado, hablamos de una VLAN (Virtual LAN). También cabe mencionar las SAN (Storage Área Network), concebida para conectar servidores y matrices de discos y las Redes Irregulares, donde los cables se conectan a través de un módem para formar una red.

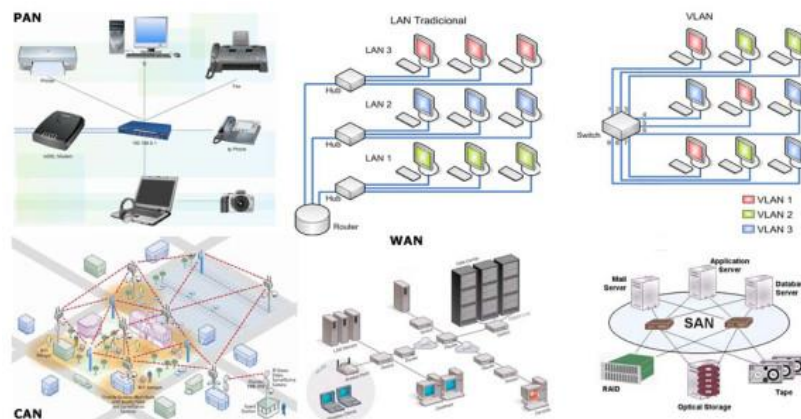


Figura 2

1.4.2 Redes Por Tipo De Conexión.

Cuando hablamos de redes por tipo de conexión, el tipo de red varía dependiendo si la transmisión de datos es realizada por medios guiados como cable coaxial, par trenzado o fibra óptica, o medios no guiados, como las ondas de radio, infrarrojos, microondas u otras transmisiones por aire.

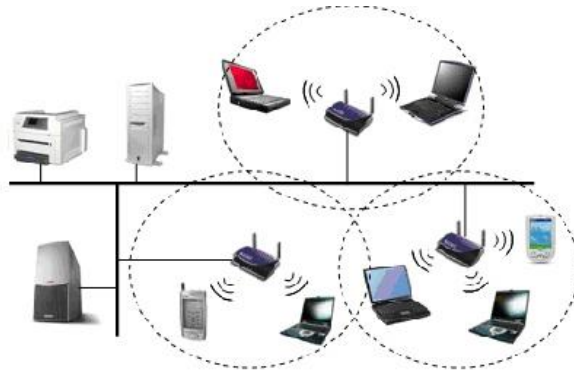


Figura 3

En la imagen de WLAN (Wireless LAN) podemos ver el medio “guiado” representado por la línea negra de cableado, y el medio “no guiado”, correspondiente al acceso inalámbrico marcado en los círculos punteados.

1.4.3 Redes Por Relación Funcional.

Cuando un cliente o usuario solicita la información a un servidor que le da respuesta es una Relación Cliente/Servidor, en cambio cuando en dicha conexión una serie de nodos operan como iguales entre sí, sin cliente ni servidores, hablamos de Conexiones Peer to Peer o P2P.

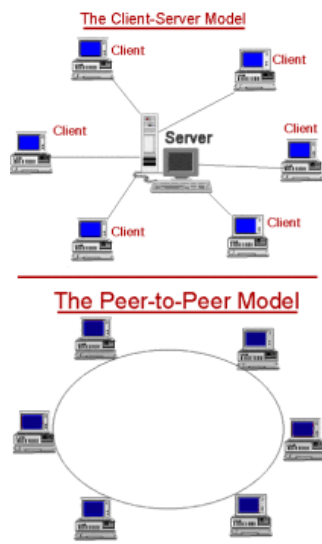


Figura 4

1.4.4 Redes Por Topología.

La Topología de una red, establece su clasificación en base a la estructura de unión de los distintos nodos o terminales conectados. En esta clasificación encontramos las redes en bus, anillo, estrella, en malla, en árbol y redes mixtas.

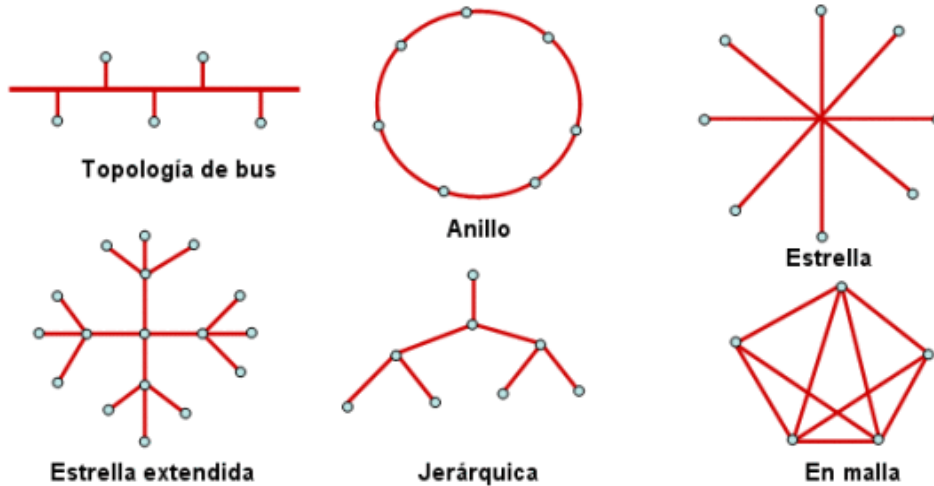


Figura 5

1.4.5 Redes Por Direccionalidad De Datos.

En la direccionalidad de los datos, cuando un equipo actúa como emisor en forma unidireccional se llama Simplex, si la información es bidireccional pero solo un equipo transmite a la vez, es una red Half-Duplex o Semi-Duplex, y si ambos equipos envían y reciben información simultáneamente hablamos de una red Full Duplex.

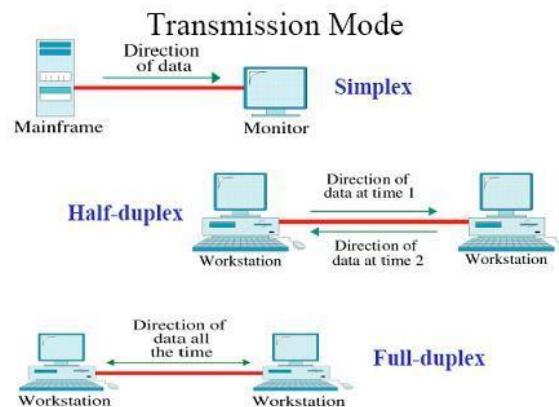


Figura 6

1.4.6 Redes Según Grado De Autentificación.

Las Redes Privadas y la Red de Acceso Público, son 2 tipos de redes clasificadas según el grado de autentificación necesario para conectarse a ella. De este modo una red privada requiere el ingreso de claves u otro medio de validación de usuarios, una red de acceso público en cambio, permite que dichos usuarios accedan a ella libremente.

1.4.7 Según Grado De Difusión.

Otra clasificación similar a la red por grado de autentificación, corresponde a la red por Grado de Difusión, pudiendo ser Intranet o Internet. Una intranet, es un conjunto de equipos que comparte información entre usuarios validados previamente, Internet en cambio, es una red de alcance mundial gracias a que la interconexión de equipos funcionan como una red lógica única, con lenguajes y protocolos de dominio abierto y heterogéneo.

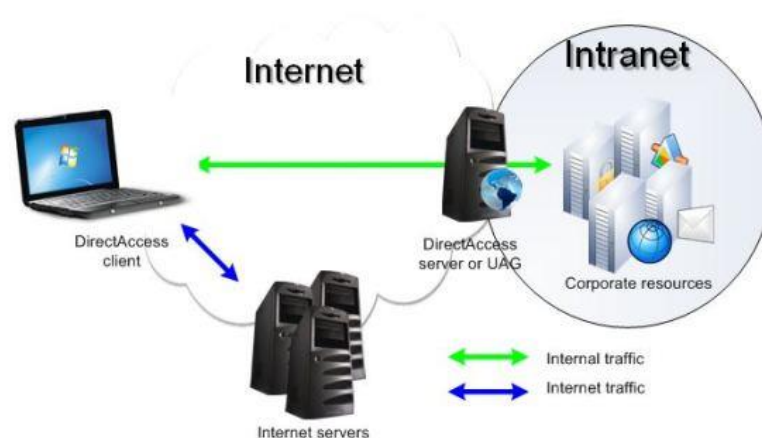


Figura 7

1.4.8 Redes Según Servicio o Función.

Por último, según Servicio o Función de las Redes, se pueden clasificar como Redes Comerciales, Educativas o Redes para el Proceso de Datos.

Todas estas clasificaciones, nos permiten identificar la forma en que estamos conectados a una red, qué uso podemos darle y el tipo de información a la cual tendremos acceso. Conocerlas entonces nos servirá para elegir con una base mucho más sólida, qué conexión necesitamos para cubrir las necesidades de nuestro negocio y valorizar los costos que implica cada una de ellas.

1.5 Importancia de las redes en la actualidad.

Hoy en día las redes informáticas se utilizan en abundancia para interconectar recursos entre diferentes computadoras. Estos recursos, pueden ser tanto de hardware como de software. Un ejemplo del primero puede ser una impresora que la usen diferentes usuarios por diversas computadoras.

1.6 Ventajas de las redes informáticas:

- Una de las principales ventajas de las redes informáticas es que la velocidad de transmisión es muy rápida.
- Es posible comprar un solo periférico y conectarlo en red con muchas computadoras para no gastar mucho dinero comprando un periférico por ordenador. Un ejemplo sería comprar una impresora y conectarla en red con muchas computadoras.
- Cuando se está trabajando con bases de datos, se necesita que la información puesta en estas se actualice correctamente; y de esta forma se pueden utilizar las redes informáticas para que muchas computadoras no tengan datos desactualizados en las bases de datos.

En conclusión una red de ordenadores posibilita:

1. Mayor facilidad en la comunicación entre usuarios.
2. Reducción en el presupuesto para software y hardware.
3. Organización de los grupos de trabajo que la conforman.
4. Mejoras en la administración de los equipos y programas.
5. Mejoras en la integridad de los datos.
6. Mayor seguridad para acceder a la información.

Capítulo 2 Concepto e Historia de IPV6.

2.1 Concepto de IPv6.

IPv6 (Internet Protocol Version 6) o IPng (Next Generation Internet Protocol) es la nueva versión del protocolo IP (Internet Protocol). Ha sido diseñado por el IETF (Internet Engineering Task Force) para reemplazar en forma gradual a la versión actual, el IPv4.

En esta versión se mantuvieron las funciones del IPv4 que son utilizadas, las que no son utilizadas o se usan con poca frecuencia, se quitaron o se hicieron opcionales, agregándose nuevas características.

2.2 ¿Por qué surge?

El motivo básico para crear un nuevo protocolo fue la falta de direcciones. IPv4 tiene un espacio de direcciones de 32 bits, en cambio IPv6 ofrece un espacio de 128 bits. El reducido espacio de direcciones de IPv4, junto al hecho de falta de coordinación para su asignación durante la década de los 80, sin ningún tipo de optimización, dejando incluso espacios de direcciones discontinuos, generan en la actualidad, dificultades no previstas en aquel momento.

Otros de los problemas de IPv4 es la gran dimensión de las tablas de ruteo en el backbone de Internet, que lo hace ineficaz y perjudica los tiempos de respuesta.

Debido a la multitud de nuevas aplicaciones en las que IPv4 es utilizado, ha sido necesario agregar nuevas funcionalidades al protocolo básico, aspectos que no fueron contemplados en el análisis inicial de IPv4, lo que genera complicaciones en su escalabilidad para nuevos requerimientos y en el uso simultáneo de dos o más de dichas funcionalidades. Entre las más conocidas se pueden mencionar medidas para permitir la Calidad de Servicio (QoS), Seguridad (IPsec) y movilidad.

2.3 Situación actual

Los principales proveedores de servicios de Internet (ISP), el hogar de redes y fabricantes de equipos, empresas de Internet de todo el mundo se están uniendo para habilitar permanentemente IPv6 para sus productos y servicios.

En el año transcurrido desde Lanzamiento Mundial de IPv6 comenzó el 6 de junio de 2012, la utilización mundial de IPv6 se ha duplicado. 2013 marca el tercer año consecutivo que el consumo IPv6 en la Internet mundial se ha duplicado. Si las tendencias actuales continúan, más de la mitad de los usuarios de Internet de todo el mundo estarán en IPv6 conectadas en menos de 6 años.

2.4 Historia de IPv6

- Para el invierno de 1992 la comunidad del Internet había desarrollado cuatro propuestas diferentes para el IPng que eran: CNAT, IP Encaps, Nimrod y Simple CLNP.
- Después para diciembre del mismo año, aparecieron tres propuestas más el " PIP " (The P Internet Protocol), el " SIP " (The Simple Internet Protocol) y el " TP/IX".
- En la primavera de 1992 el "Simple CLNP" se desarrolló en el " TUBA" (TCP and UDP with Bigger Addresses" , y el " IP Encaps " en " IPAE " (IP Address Encapsulation)
- Para el verano de 1993, IPAE se combinó con el SIP aunque mantuvo el nombre SIP, que posteriormente se fusionó con la PIPA, y al grupo de trabajo resultante se le llamó "SIPP" (Simple Internet Protocol Plus). Casi al mismo tiempo el grupo de trabajo TP/IX cambió su nombre por el de "CATNIP" (Common Architecture for the Internet)
- Posteriormente, en la reunión del IETF del 25 de julio de 1994 en Toronto Canadá, los directores de área del mismo organismo recomendaron el uso del IPng y lo documentaron en el RFC 1752, (la recomendación para el protocolo IP de siguiente generación)
- El 17 de noviembre del mismo año fue aprobada esta recomendación por el "IESG" (Internet Engineering Steering Group) que elaboró una propuesta de estándar o norma.

2.5 IPv6 en México.

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

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

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

En octubre del 2000 se obtuvo un bloque del tipo sTLA (2001:0448::/35), adjudicado por ARIN, la entidad de registro para Norteamérica y que en aquel entonces daba servicio también a Latinoamérica, que se ha utilizado por ejemplo en la RedCUDI, la red de Internet2 de México.

Posteriormente, en junio de 2005 se obtiene otro bloque de direcciones IPv6 adjudicado por LACNIC, la entidad de registro para Latinoamérica y el Caribe.

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 en agosto de 1999. Esta red contó con varios túneles hacia otros nodos de Backbone de 6Bone: SPRINT, FIBERTEL, MERIT, BAY NETWORKS, JANET e ISI-LAP, y hacia los hosts que ha tenido la UNAM corriendo con distintos sistemas operativos como Windows 2000, 2003, Vista y 7, Solaris, varias distribuciones de Linux y de BSD.

Actualmente se sigue trabajando con instituciones mexicanas y de América Latina para realizar su conexión IPv6 hacia la UNAM. Entre las instituciones mexicanas han destacado: Instituto Politécnico Nacional, Universidad Autónoma Metropolitana, Instituto Tecnológico de Estudios Superiores de Monterrey, Universidad Autónoma de Chiapas, Universidad Autónoma de Guerrero, Universidad Autónoma del Estado de Hidalgo, Universidad Autónoma de Nuevo León, Instituto Tecnológico de Oaxaca, Instituto Tecnológico de Mérida, Instituto Tecnológico Autónomo de México, PEMEX, STYX, ASTER, etc.

Entre las instituciones latinoamericanas han estado: Instituto de Informática de la Universidad Austral de Chile y las universidades UBio-Bio, UFRO y UDLA; ex-RETINA ahora InnovaRed, y las universidades LINTI-UNLP, UBA, de Argentina; EAFIT y las universidades UdeA, UniCauca y UniPamplona de Colombia; INICTEL, NITCOM, y la UNI de Perú, etc.

En enero del 2010 se pone en funcionamiento un servidor de Túneles para ofrecer conexión automática con IPv6 en RedUNAM y salir a Internet también con IPv6.

El 8 de junio de 2011, declarado como “Día Mundial de IPv6” o “IPv6 World Day” por la Internet Society (ISOC, por sus siglas en inglés), durante 24 horas la UNAM participó en este evento mundial mediante la habilitación de IPv6 en su portal principal (www.unam.mx), al cual pudieron acceder todos los usuarios de manera transparente tanto por IPv4 como por IPv6.

2.6 Características principales

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits, para soportar: más niveles de jerarquías de direccionamiento y más nodos direccionables.
- 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 procesamiento 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.
- Capacidad de etiquetas de flujo. Puede ser usada por un nodo origen para etiquetar paquetes pertenecientes a un flujo (flow) 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.
- Autoconfiguración: la autoconfiguración de direcciones es más simple. Especialmente en direcciones Agregatable Global Unicast, los 64 bits superiores son seteados por un mensaje desde el router (Router Advertisement) y los 64 bits más 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 más simple.
- 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

2.7 ¿Qué tan grande es el espacio de direcciones?

Habrían 2^{128} direcciones IP diferentes, significa que si la población mundial fuera de 10 billones habría $3.4 \cdot 10^{27}$ direcciones por persona. O visto de otra forma habría un promedio de $2.2 \cdot 10^{20}$ direcciones por centímetro cuadrado. Siendo así muy pequeña la posibilidad de que se agoten las nuevas direcciones.

2.7.1 Direccionamiento

Las direcciones son de 128 bits e identifican interfaces individuales o conjuntos de interfaces. Al igual que en IPv4 en los nodos se asignan a interfaces.

Se clasifican en tres tipos:

- *Unicast* identifican a una sola interfaz. Un paquete enviado a una dirección unicast es entregado sólo a la interfaz identificada con dicha dirección. [\[RFC 2373\]](#) [\[RFC 2374\]](#)
- *Anycast* identifican a un conjunto de interfaces. Un paquete enviado a una dirección anycast, será entregado a alguna de las interfaces identificadas con la dirección del conjunto al cual pertenece esa dirección anycast. [\[RFC 2526\]](#)
- *Multicast* identifican un grupo de interfaces. Cuando un paquete es enviado a una dirección multicast es entregado a todos las interfaces del grupo identificadas con esa dirección.

En el IPv6 no existen direcciones broadcast, su funcionalidad ha sido mejorada por las direcciones multicast. [\[RFC 2375\]](#)

2.7.1.2 Representación de las direcciones

Existen tres formas de representar las direcciones IPv6 como strings de texto.

- $x:x:x:x:x:x$ donde cada x es el valor hexadecimal de 16 bits, de cada uno de los 8 campos que definen la dirección. No es necesario escribir los ceros a la izquierda de cada campo, pero al menos debe existir un número en cada campo.

Ejemplos:

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

- Como será común utilizar esquemas de direccionamiento con largas cadenas de bits en cero, existe la posibilidad de usar sintácticamente :: para representarlos. El uso de :: indica uno o más grupos de 16 bits de ceros. Dicho símbolo podrá aparecer una sola vez en cada dirección.

Por ejemplo:

1080:0:0:0:8:800:200C:417A	unicast address
FF01:0:0:0:0:0:101	multicast address
0:0:0:0:0:0:1	loopback address
0:0:0:0:0:0:0	unspecified addresses

Podrán ser representadas como:

1080::8:800:200C:417A	unicast address
FF01::101	multicast address
::1	loopback address
::	unspecified addresses

- Para escenarios con nodos IPv4 e IPv6 es posible utilizar la siguiente sintaxis:

x:x:x:x:x:d.d.d.d, donde x representan valores hexadecimales de las seis partes más significativas (de 16 bits cada una) que componen la dirección y las d, son valores decimales de los 4 partes menos significativas (de 8 bits cada una), de la representación estándar del formato de direcciones IPv4.

Ejemplos:

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

o en la forma comprimida

```
::13.1.68.3
::FFFF:129.144.52.38
```

2.7.1.2 Representación de los prefijos de las direcciones

Los prefijos de identificadores de subredes, routers y rangos de direcciones IPv6 son expresados de la misma forma que en la notación CIDR utilizada en IPv4. Un prefijo de dirección IPv6 se representa con la siguiente notación:

Direccion-ipv6/longitud-prefijo, donde

Direccion-ipv6: es una dirección IPv6 en cualquiera de las notaciones mencionadas anteriormente.

longitud-prefijo: es un valor decimal que especifica cuantos de los bits más significativos, representan el prefijo de la dirección.

Direcciones Global Unicast

Formato de las direcciones global unicast



Figura 8

Prefijo de ruteo global: es un prefijo asignado a un sitio, generalmente está estructurado jerárquicamente por los RIRs e ISPs.

Identificador de Subred: es el identificador de una subred dentro de un sitio. Está diseñado para que los administradores de los sitios lo estructuren jerárquicamente

Identificador de Interfaz: es el identificador de una interfaz. En todas las direcciones unicast, excepto las que comienzan con el valor binario 000, el identificador de interfaz debe ser de 64 bits y estar construido en el formato Modified EUI-64.

El formato para este caso es el siguiente:

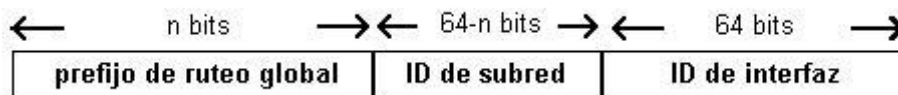


Figura 9

El siguiente es un ejemplo del formato de direcciones global unicast bajo el prefijo 2000::/3 administrado por el IANA

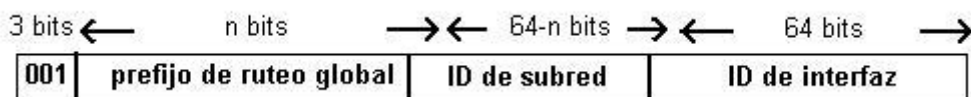


Figura 10

La asignación del espacio de direcciones IPv6 global unicast está accesible en [IPV6 GLOBAL UNICAST ADDRESS ASSIGNMENTS](#)

2.8 DNS

El almacenamiento actual de direcciones de Internet en el Domain Name System (DNS) de IPv4 no se puede extender fácilmente para que soporte direcciones IPv6 de 128 bits, ya que las aplicaciones asumen que a las consultas de direcciones se retornan solamente direcciones IPv4 de 32 bits.

Para poder almacenar las direcciones IPv6 se definieron las siguientes extensiones (ver [RFC 3596](#))

- un nuevo tipo de registro, el registro AAAA. Se usa para almacenar direcciones IPv6, porque las extensiones están diseñadas para ser compatibles con implementaciones de DNS existentes;
- un nuevo dominio para soportar búsquedas basadas en direcciones IPv6. Este dominio es IP6.ARPA;
- Redefinición de las consultas existentes, que localizan direcciones IPv4, para que puedan también procesar direcciones IPv6.

Los cambios son diseñados para ser compatibles con el software existente. Se mantiene el soporte de direcciones IPv4.

2.9 Mecanismos de transición básicos

Los mecanismos de transición son un conjunto de mecanismos y de protocolos implementados en hosts y routers, junto con algunas guías operativas de direccionamiento designadas para hacer la transición de Internet al IPv6 con la menor interrupción posible.

Existen dos mecanismos básicos:

- *Dual Stack*: provee soporte completo para IPv4 e IPv6 en host y routers.
- *Tunneling*: encapsula paquetes IPv6 dentro de headers IPv4 siendo transportados a través de infraestructura de ruteo IPv4.

Dichos mecanismos están diseñados para ser usados por hosts y routers IPv6 que necesitan interoperar con hosts IPv4 y utilizar infraestructuras de ruteo IPv4. Se espera que muchos nodos necesitarán compatibilidad por mucho tiempo y quizás indefinidamente. No obstante, IPv6 también puede ser usado en ambientes donde no se requiere interoperabilidad con IPv4. Nodos diseñados para esos ambientes no necesitan usar ni implementar estos mecanismos.

2.9.1 Dual Stack

La forma más directa para los nodos IPv6 de ser compatibles con nodos IPv4-only es proveyendo una implementación completa de IPv4. Los nodos IPv6 que proveen una implementación completa de IPv4 (además de su implementación de IPv6) son llamados nodos "IPv6/IPv4". Estos nodos tienen la habilidad de enviar y recibir paquetes IPv6 e IPv4, pudiendo así interoperar directamente con nodos IPv4 usando paquetes IPv4, y también operar con nodos IPv6 usando paquetes IPv6.

2.9.2 Tunneling

Los nodos o redes IPv6 que se encuentran separadas por infraestructuras IPv4 pueden construir un enlace virtual, configurando un túnel. Paquetes IPv6 que van hacia un dominio IPv6 serán encapsulados dentro de paquetes IPv4. Los extremos del túnel son dos direcciones IPv4 y dos IPv6. Se pueden utilizar dos tipos de túneles: configurados y automáticos. Los túneles configurados son creados mediante configuración manual. Un ejemplo de redes conteniendo túneles configurados es el 6bone. Los túneles automáticos no necesitan configuración manual. Los extremos se determinan automáticamente usando direcciones IPv6 IPv4-compatible.

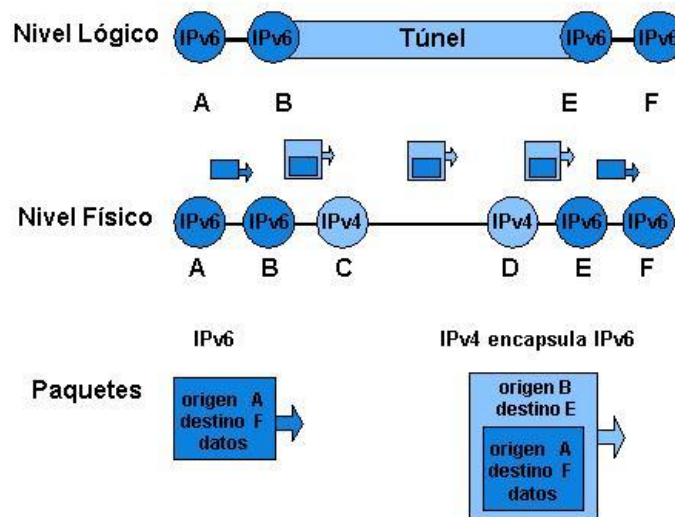


Figura 11

Capítulo 3 Análisis y Diseño de la Red.

3.1 Diseño de la red

Se considera un diseño de red previo en la que se analizaran los diferentes factores que puedan influir en el desempeño de la nueva red, algunos a tomar en cuenta son la compatibilidad de isp, la intranet, equipos existentes. Topología que usa mismos que iremos mencionando para hacer énfasis en el rol que juegan en el diseño de la red ipv6.

3.2 Características a considerar de la red

La red existente es una red ipv4 en cascadeo, con IP's estáticas versión 4. Esta red cuenta con 230 nodos la cual cubre las comunicaciones entre las áreas sistemas, personal, compras, contabilidad, estadística, archivo clínico, mantenimiento, seguridad, damas voluntarias, consulta externa, cirugía plástica, medicina general, captación de fondos, voluntariado, transportes, dirección operativa, juventud, centro de sangre, escuela de enfermería, rayos x, laboratorio, área de trauma, área de cirugía, laboratorio de sangre, terapia intensiva, inhaloterapia, psicología, sicoa, ciu, torre de radio, trabajo social, caja, hospitalización, servicios generales, dirección médica, dirección de administrativa y finanzas, presidencia, subdirección médica, auditoría, auditoría médica, enseñanza, biblioteca, enfermería, donación de órganos, almacén, farmacia, rehabilitación, central de equipos y ISO.

Esta red cubre la función de mantener en comunicación todas las áreas debido a la constante capacitación por parte del sistema de gestión de calidad (ISO) ya que por medio de la red se les hacen llegar de manera digital los manuales, también se concentra la información mediante diferentes servidores para cada área en específico, permitiendo solo el acceso a estos a las áreas que lo requieren.

Esta red se comunicara con la otra red mediante un túnel en ipv4, este permitirá la coexistencia entre la 2 redes, en esta sección se puede presentar un problema que es el conmutar por un túnel en ipv4, se usara el mecanismo de transición: 1. 6PE sobre MPLS (Cisco, 2002), el cual permite que los sitios IPv6 se comuniquen usando caminos conmutados de etiquetas sobre un núcleo MPLS IPv4., esto para la comunicación de intranet.

Hablando de nuestro ISP podemos decir que no tendremos problemas, puesto que es compatible con ipv6 lo cual permitirá la conexión de manera transparente para el enlace externo a la nube de internet.

3.3 Descripción de la nueva red.

Archivo clínico tiene la necesidad de crecer debido a que es necesario cumplir con la norma NOM-024-SSA3-2010 que estipula que todas las instituciones del área de la salud deben contar con un expediente de tipo electrónico, para lo que la cruz roja mexicana iap delegación distrito federal adquirió un software a la medida y requiere de una nueva red para uso exclusivo del mismo, considerando que a esta nueva red se tendrán que implementar 50 equipos de cómputo, con miras a que se incrementen la cantidad de los mencionados.

Por lo antes mencionado la capacidad de la red anterior es sobrepasada. Puesto que cuenta con 230 equipos y es una red clase C con una máscara de subred 255.255.255.0 y obliga buscar una solución al área encargada que es sistemas.

Nosotros sugerimos el desarrollo de una red en ipv6 que pudiera coexistir con una red de ipv4, que a su vez permitiera crear una sola red de manera híbrida. A lo que el jefe del área de sistemas José Luis Gómez Soriano respondió diciendo que sería viable la implementación del proyecto, como solución al problema del expediente electrónico y en futuro a la escases de IP's en toda la institución.

3.3.1 Cobertura de la red

Las áreas dentro de la cruz roja iap delegación distrito federal que tengan que ver directamente con el área médica tendrán acceso a esta red, también instituciones del mismo rubro que la cruz roja, tendrán acceso a esta red por medio de internet , tal como lo pide la norma NOM-024-SSA3-2010.

3.3.2 Necesidades

Dentro de las necesidades que tiene esta nueva red están el concentrar información en un servidor .al cual se tendrá acceso por medio de software. También los equipos tendrán la manera de comunicarse entre sí por medio de una intranet y necesitan los equipos tener acceso internet para actualización de software, y comunicación con otras instituciones.

3.3.3 Topología

Dado que la primera red utiliza la arquitectura en cascadeo será la misma que utilizaremos para la nueva red ya que se nos solicitó por parte del ingeniero José Luis Gómez Soriano, que implementáramos esta con la finalidad de facilitar la capacitación y desempeño del área de soporte.

3.3.4 Metodología

Los elementos constitutivos del modelo son: el establecimiento de una conexión IPv6 entre las oficinas remotas y la red de la oficina central mediante 6PE para obtener una Intranet IPv6nativa; proveer el servicio de Internet IPv6 a la Intranet mediante 6to4; conservar el acceso al servicio Internet IPv4 para la Intranet mediante el uso de NAT64 y DNS64

3.3.4.1 Conexión a internet

El principal inconveniente para utilizar IPv6 de forma nativa en la oficina central de una red corporativa (red interna o red de campus), es que IPv6 no está ampliamente implementado en las redes de los ISP, entonces si se implementa IPv6 de forma nativa en la oficina central de una red corporativa y el ISP no provee conexión directa para este protocolo, la red de la oficina central perdería toda conectividad externa, esto incluye Internet y la conexión a oficinas remotas, incluso si estas son compatibles con IPv6. Para solucionar este problema se pueden utilizar los siguientes dos mecanismos de transición: 1. 6PE sobre MPLS (Cisco, 2002), el cual permite que los sitios IPv6 se comuniquen usando caminos conmutados de etiquetas sobre un núcleo MPLS IPv4. 2. Túnel 6to4 (Carpenter & Moore, 2001), el cual es un mecanismo de túnel automático que usa infraestructura IPv4 para permitir la comunicación de dominios IPv6. Como consecuencia de esta solución se pierde conectividad a Internet IPv4, lo cual hace necesario utilizar como tercer mecanismo de transición a NAT64 (Bagnulo et al., 2011a), el cual se encarga de trasladar los datagramas IPv6 a IPv4, en conjunto con el mecanismo DNS64 (Bagnulo et al., 2011b) que permite la resolución de nombres. Estos mecanismos permitirán la implementación de IPv6 de forma nativa en la oficina central sin que se pierdan sus conexiones externas. En la figura 1 se presenta la red diseñada, en la cual se tiene una red IPv6 nativa con tres encaminadores de borde, uno para la conexión con oficinas remotas "R2. IPv6", otro para la conexión a Internet IPv6 "R. 6TO4" y finalmente uno para conexión con Internet IPv4 "R. NAT64", en la tabla 1 se presentan las direcciones de los dispositivos de la red que intervienen en el proceso de transición.

3.3.4.2 Conexión con las oficinas remotas

Las alternativas estáticas existentes para transportar IPv6 sobre un túnel IPv4 y dar servicio IPv6 a las oficinas remotas son túnel configurado manualmente e IPv6 sobre túnel GRE IPv4. Estas opciones son difíciles de gestionar cuando el número de oficinas aumenta, especialmente en topologías completamente enmalladas. Las alternativas dinámicas son: 1. Tunnel Broker, requiere que el servicio soporte cambios remotamente y tiene implicaciones de seguridad. 2. Túnel 6to4, debido a que la dirección IPv4 pública subyacente determina el valor de los 32 bits siguientes al prefijo 2002::/16, una futura migración en la que se requiera que IPv6 sea el único protocolo de red (a lo cual se le denomina IPv6 nativa o IPv6-only) requiere un cambio en la numeración de las direcciones IPv6. 3. IPv6 sobre MPLS, usa la infraestructura MPLS existente y puede ser dispendioso de configurar dependiendo del método subyacente utilizado (IPv6 en circuitos de transporte sobre MPLS, IPv6 usando túneles IPv4 en los encaminadores de borde de usuario o IPv6 con núcleo MPLS basado en IPv4 “6PE/6VPE”). Para el camino 1 de red entre los equipos “R2. IPv6” y “R3 IPv6” de la figura 1 se presenta la alternativa seleccionada para solucionar la conexión con las oficinas remotas IPv6, la cual consiste en la implementación por parte del ISP del mecanismo 6PE sobre MPLS; este mecanismo consiste en activar el intercambio de rutas IPv6 entre los encaminadores de borde del proveedor. La ventaja de este mecanismo es que no requiere la realización de cambios en el núcleo MPLS ya que una vez el datagrama IPv6 llega a los equipos 6PE, es encapsulado dentro de MPLS y el encaminamiento se hace a nivel de etiquetas.

3.3.4.1 Conexión a Internet IPv4

La razón principal por la que se implementa IPv6 en escenarios de doble pila es para poder seguir utilizando los servicios que actualmente se prestan con IPv4; hay que reconocer que aunque IPv6 es superior en muchos sentidos a IPv4, la mayoría de servicios que actualmente se prestan en la Internet lo hacen bajo IPv4, y no resulta aceptable implementar una red que no pueda acceder a estos servicios. Para resolver esta necesidad se implementó el mecanismo NAT64 en combinación con DNS64 representados en la figura 2. Este mecanismo de traducción le permite a la red IPv6 nativa diseñada, acceder a servicios de la Internet IPv4, evitando así los inconvenientes que se presentan en una red doble pila.

El mecanismo NAT64 funciona por medio de un servidor DNS64 que recibe las consultas de clientes IPv6, el servidor DNS64 a su vez se comunica con otros servidores DNS (Albitz & Liu, 2006) ubicados en Internet. Cuando la consulta corresponde a un nombre de host que tiene dirección IPv4, el DNS64 transforma esta dirección en una dirección IPv6 anteponiéndole el prefijo que identifica el servicio NAT64. La red debe estar configurada de tal forma que los paquetes enviados a un destino que contenga el prefijo del NAT64, utilicen el encaminador NAT64 como puerta de enlace, la función de este encaminador es convertir paquetes IPv6 en paquetes IPv4 y viceversa.

El servidor DNS64 debe comunicarse con otros servidores DNS IPv4 para resolver nombres de dominios. Puesto que el servidor DNS64 se encuentra en la red IPv6 nativa, se le realizó a éste una modificación que consistió en configurar las direcciones de los servidores DNS IPv4 externos como direcciones IPv6 utilizando el prefijo del NAT64, de esta manera cuando el servidor DNS64 necesite realizar una consulta a un DNS IPv4, lo hará mediante IPv6 utilizando al encaminador NAT64 como puerta de enlace y éste se encargará de realizar las traducciones correspondientes.

En la implementación de este escenario se utilizó el servidor de nombres de dominio de Internet de Berkeley BIND para proveer los servidores DNS64 y DNS (Internet Systems Consortium, 2012) de la figura 2. Para implementar el encaminador NAT64, se utilizó un desarrollo de la firma Viagénie denominado “Ecdysis: opensource implementation of a NAT64 gateway”, el cual permite habilitar una estación para que realice las funciones de este encaminador. El encaminador NAT64 que se implementó dentro de una estación, es un mecanismo relativamente nuevo que se encuentra implementado solamente en encaminadores modernos.

Para activar el funcionamiento de DNS64 se debe adicionar al archivo de opciones del servidor BIND la configuración presentada en la figura 5. Para activar el funcionamiento del encaminador NAT64, basta con descargar el disco compacto “cd-live” que se encuentra disponible en Viagénie (2010), configurar las direcciones IPv4 e IPv6 sobre las interfaces de la estación y ejecutar el script de configuración “nat64-config.sh” que se encuentra dentro del “cd-live”.

Capítulo 4 Concepto de virtualización y pruebas.

Una vez se tomaron las características de diseño de la red, procederemos a la implementación de esta red es necesario ser muy cuidadosos para evitar cualquier afectación a la red anterior pues la misma es la espina dorsal de la información en la institución. Por lo tanto la fase de la implementación estará dividida en dos grandes fases una la virtualización de la red a implementar, misma que se implementara con la finalidad de testear la red en ipv6 para ver que no hay problemas de coexistencia. y la segunda la implementación física, en donde se instalara en los routers el software necesario y se dará de alta la ipv6 en los equipos

4.1 Virtualización de la red.

Hoy en día, las empresas tanto del sector público como el privado están inmersas en un mundo competitivo en el que es necesario revisar y renovar los modelos de trabajo tradicionales en cuestión de calidad. Las tecnologías de la información brindan la posibilidad de definir nuevas estrategias de trabajo mucho más eficientes y efectivas, valiéndose de la tecnológica y sus avances. La virtualización es uno de los más fuertes y con mayor crecimiento con el paradigma de la nube en estos años “La investigación mostró que muchas de las empresas ya han adoptado la virtualización de servidores (72%) como parte de su estrategia para reducir costes y crecer en flexibilidad. El almacenamiento y la virtualización de aplicaciones también se están usando pero en menor medida – alrededor de la mitad de las empresas entrevistadas. “(COLT telecom, 2007).

Estos recursos informáticos abarca la creación de una plataforma informática formada por réplicas de computadores “reales” que son creados a base de software. Respetando sus características tipos y usos. Pero reduciendo costes como espacio y recursos.

4.1.1 Generalidades de la virtualización

Producto del mundo globalizado en el que vivimos, nos encontramos que las instituciones han venido experimentando cambio significativo en sus procesos y en la forma en cómo se llevan a cabo las relaciones con sus clientes, proveedores y colaboradores. Con la expansión de las redes de información y los adelantos continuos en el campo tecnológico, tanto a nivel de hardware como de software, han producido que estas adopten la gran tarea de aprovechar toda esta innovación tecnológica en pro de mejorar su comunicación , lograr automatizar la mayor cantidad de sus procesos , y beneficiar a sus empleados la posibilidad de acceder a la información y a la infraestructura que requieren para tener Capacidad de respuesta a los nuevos retos y oportunidades que se dan.

Paralelamente, dentro de toda esta gama de oportunidades de mejora que se presentan con las tecnologías de información (conocidas como TI), relacionados con la posibilidad de ofrecer a sus empleados recursos seguros y confiables, que permitan simular el comportamiento organizacional diario que ejecutan desde su oficina, solo que se logre mediante un acceso distribuido. Las proyecciones fijadas en las nuevas tecnologías y su potencial de apoyo se fundamentan en poder contar con herramientas que sean ágiles fáciles de usar, así como confiables y con alto porcentaje de disponibilidad, buscando superar a los problemas de altos costos, innovación y de seguridad y asuntos legales. Es por eso, que este desafío para las empresas implica reducir la resistencia al cambio de contar con infraestructuras tecnológicas flexibles y adaptadas a las necesidades de la propia empresa, en busca de alcanzar éxito en sus operaciones diarias sin sacrificar la seguridad de los datos en la institución.

Este tipo de tecnologías se enfocan en el concepto de la virtualización, la idea enfocada en contar con redes de información más eficientes, adaptables y que sean congruentes con los objetivos estratégicos de la organización que ponga en práctica este enfoque. Aspectos como contar con una mejor comunicación empresarial, elevar la productividad del trabajo realizado, entre otros que se abordarán más adelante, impulsan a calificar a la virtualización como una modalidad que está empezando a ser moda en las organizaciones hoy en día, y que les sirven de mucho en su proceso de transformación tecnológica.

4.1.2 Definición de virtualización

El concepto de virtualización nace con la idea de mejorar la utilización de recursos tecnológicos mediante una agrupación común de éstos y que se pueden llegar compartir con cualquier persona en el mundo. Estos recursos tecnológicos podrían incluir los servidores, servicios de almacenamiento y trabajo en redes como la Internet. De esta forma, mediante la virtualización los recursos pueden ser ubicados dinámicamente a través de las aplicaciones y procesos de una organización, siendo así una técnica que es utilizada para ocultar las características físicas de los recursos de una computadora, con relación a la forma en que otros sistemas, aplicaciones y/o usuarios interactúan con los recursos. En otras palabras, la virtualización aprovecha sus capacidades por las cuales fue creada, para brindar a un usuario o empresa servicios tecnológicos mediante interfaces de simulación entre lo que es hardware y software (a nivel del sistema operativo y también aplicaciones). Básicamente, la idea es sustituir la parte del hardware de computadora por un software que emule mediante una máquina virtual que es la que se encarga de hacer el acople entre el hardware existente y los diferentes sistemas operativos que interactúan con los recursos, y sobre las aplicaciones que corren sobre los sistemas operativos. Con ello, se busca que la gestión del manejo de la virtualización traiga consigo un uso más eficiente de los recursos de TI y una mayor flexibilidad para proporcionar los recursos de computación en el momento y lugar que se necesitan.

La enciclopedia Wikipedia en su sitio en Internet define virtualización como:

“En informática, **virtualización** es un término amplio que se refiere a la abstracción de los recursos de una computadora. Este término es bastante antiguo: viene siendo usado desde antes de 1960, y ha sido aplicado a diferentes aspectos y ámbitos de la informática, desde sistemas computacionales completos hasta capacidades o componentes individuales.”

El término en sí se ha aplicado desde hace muchos años, cuando IBM fue el pionero en su implementación, utilizando máquinas virtuales para computadoras mainframe, y conforme han pasado los años, ha ido junto con otras empresas tecnológicas- adaptando este concepto a los diferentes necesidades que se han ido generando en distintos contextos tecnológicos a través de los años y hasta la actualidad.

En resumen, en un ambiente virtualizado, las funciones lógicas de la computadora, el almacenamiento y los elementos de red son separados de sus funciones físicas, pasando a ser agrupados virtualmente, y en donde esos elementos podrían ser localizados manual o automáticamente para satisfacer las necesidades de cambio y prioridades de negocio. La virtualización le ayuda a un negocio a transformar su ambiente de TI en una infraestructura adaptable, en donde le va a permitir brindar aplicaciones y servicios de negocios más rápidamente, poner en uso recursos de almacenamiento desperdiciados hasta ahora, destacando las prioridades como negocio y creciendo en disponibilidad, seguridad y continuidad del mismo.

4.1.3 Tipos de virtualización

Como se ha venido comentando, la virtualización se puede aplicar de distintas formas y en distintos ambientes. En la tabla 1 se resumen las características principales de cada uno de estos tipos de virtualización que se pueden implementar.

Tabla 1

Resumen de los tipos de virtualización y sus características principales	
Tipo de virtualización	Características
Virtualización de almacenamiento	Es aquella en donde se unen múltiples dispositivos de almacenamiento en red, en lo que aparenta ser una única unidad de almacenamiento. Usada en redes de área de almacenamiento, una subred de alta velocidad que comparte dispositivos de almacenamiento, y realiza tareas de almacenamiento, respaldo y recuperación de datos de forma más fácil y rápida.
Virtualización de servidor	Es en donde se particiona un servidor físico en pequeños servidores virtuales. Por ejemplo, un uso típico de esta tecnología se puede ver en los servidores Web, donde se emplean servidores virtuales para prestar servicios Web, con el objetivo principal de mantener online un sitio Web.
Virtualización a nivel de sistema operativo	El servidor físico y una única instancia del sistema operativo son virtualizadas en múltiples particiones aisladas, donde cada partición duplica un servidor real. El kernel 2 se ejecutará en un único sistema operativo y proveerá esa funcionalidad del sistema operativo para cada una de las particiones.
Virtualización de servidor local	Este tipo de virtualización se encarga de separar las aplicaciones del sistema operativo, es decir, convierte las aplicaciones en servicios virtuales gestionados y administrados de forma centralizada.
Virtualización de red	Es la segmentación o partición lógica de una única red física, para usar los recursos de la red. Trata a todos los servidores y servicios en la red como un único grupo de recursos que pueden ser accedidos sin considerar sus componentes físicos.
Diccionario informático en: http://www.alegsa.com.ar/Diccionario/diccionario.php	
2 Núcleo. Parte esencial de un sistema operativo que provee los servicios más básicos del sistema. Se encarga de gestionar los recursos como el acceso seguro al hardware de la computadora.	

4.1.4 Las razones de virtualizar.

Julia Russo califica a la virtualización como la nueva era de almacenamiento, de acuerdo a su reportaje publicado en la revista de tecnología IT Now. Para Russo (2007,57), la aplicación del término virtualización puede aplicarse tanto a nivel de software como de dispositivos de red. Sin embargo, es bajo el ambiente de los servidores de procesamiento y el almacenamiento de información en donde se logra canalizar en mayor proporción el beneficio de las reducciones de los gastos de recursos tecnológicos.

Claudio Paniagua Maciá, responsable de innovación en el área de virtualización para IBM España, Portugal, Grecia, Turquía e Israel, también tiene su aporte en cuanto a las razones importantes por las cuales virtualizar. Según su reportaje publicado en la revista Business Review, Paniagua (2006,5-6) indica que las tecnologías de virtualización solucionan satisfactoriamente los dos problemas de base que motivaron la organización en relación con los sistemas de información; a saber, compartir recursos sin crear dependencias por ello y poder definir políticas que establezcan cómo se reparte el recurso compartido. Esto, permite flexibilizar y dinamizar el sistema de información, así como maximizar la utilización de sus recursos. En un sistema de información virtualizado existen unos componentes de software “especiales” que se ubican entre las aplicaciones de negocio y los recursos físicos de la plataforma tecnológica (servidores, dispositivos de almacenamiento y redes) cuya funcionalidad es construir réplicas funcionales de los recursos físicos, llamadas recursos virtuales. Así, las aplicaciones de negocio ya no interactúan directamente con los recursos físicos, sino que lo hacen siempre con los recursos virtuales, los cuales, a su vez interactúan con los físicos.

En otras palabras, se logra de esta manera crear una nueva plataforma informática o redes de información virtuales formadas por recursos virtuales que interfiere entre las aplicaciones de emulación y la plataforma informática física original. Las aplicaciones de servicios ya no se ejecutan directamente sobre servidores físicos, sino que lo hacen sobre servidores virtuales (réplicas de ordenadores reales construidas por software).

Igualmente, las aplicaciones de servicio ya no interactúan directamente con los dispositivos de almacenamiento reales sino que lo hacen con discos virtuales, y los servidores virtuales y los discos virtuales se interconectan a través de redes virtuales y no directamente a través de la red física de comunicaciones establecida por la empresa. Analizándolo de esta manera, para las aplicaciones de servicio les es indiferente ejecutarse sobre una máquina virtual o sobre una real, acceder a una red virtual o a una real, o bien, utilizar un disco real a utilizar uno virtual. Por lo tanto, una estrategia de virtualización bien diseñada y administrada ayuda a controlar los costos, a mejorar la disponibilidad e incrementa la agilidad al evitar la complejidad que se da al tratar de tener que integrar sistemas diferentes.

Además, se trata de una tecnología que puede beneficiar a todo tipo de empresas: desde grandes multinacionales con empleados repartidos por todo el mundo hasta negocios que tan sólo tienen un servidor, como sucede en nuestro país, en donde las PYME ocupan un porcentaje muy amplio de presencia nacional, lo que sin lugar a duda se convierte en una muy buena opción para este gremio de empresas, así como para las organizaciones del sector público mexicano. Al no tener que comprar y administrar un nuevo servidor por cada nueva aplicación de servicios que se quiera poner a funcionar, o no tener que implementar o ampliar la infraestructura física de red con la que se cuenta, sino que implantar la utilización de la virtualización, se pasa a recibir una serie de ventajas como la reducción de costos, desde el punto de vista de espacio físico, consumo de energía, hardware, y algo muy importante, la mejora en el trabajo y la productividad del recurso humano de la empresa, al poder éste trabajar desde su casa o zona local, sin tener que desplazarse físicamente a su lugar de trabajo habitual diariamente.

Hoy día, se puede estimar que pocos servidores están virtualizados, a pesar del hecho de que la virtualización existe desde hace muchos años. Sin embargo, la importancia de la virtualización se ve que está aumentando a medida que las compañías presentan productos dirigidos al hardware de alto volumen y bajo costo. La razón principal es que más compañías están utilizando la virtualización para ahorrar dinero, ya que ésta logra concentrar la carga de trabajo de varios servidores en una sola máquina., con el paso del tiempo el evitar comprar más servidores para almacenar información redundante en ahorros de equipos y de energía.

De igual forma, se produce un ahorro en sueldos, ya que se cuenta con servicios fáciles de gestionar que no requieren de gran cantidad de personal. Además, también se puede ver reflejado en lo que en el pasado se requerían amplios espacios físicos para colocar los servidores, con la implementación de la virtualización se ve significativamente. El funcionamiento y operación de este tipo de tecnologías día con día ha ido simplificándose, en donde por ejemplo para las áreas de operación donde se desea instalar un nuevo servidor contable, se lo puede hacer en cuestión de minutos. De igual forma, si se quiere detener un equipo para darle mantenimiento, se pueden migrar los servidores virtuales a otro físico sin afectar la operación del negocio, lo que ayuda a que las operaciones diarias de un departamento de sistemas se simplifica significativamente. A nivel de la virtualización de aplicaciones, esta tecnología permite que se tenga la posibilidad de ejecutar en una plataforma de servidores pruebas de las nuevas versiones de software, sin afectar el sistema que se tiene corriendo normalmente.

Según Rafael Chávez, director del grupo de Sistemas Avanzados de Dell América Latina, “principalmente, la virtualización está siendo llevada hacia los servidores, porque se trata de reducir tanto espacio físico como costos». Con los servicios de virtualización que ofrecen, en Dell apuntan a simplificar las tecnologías de la información. Queremos disminuir la complejidad de la IT al hacer que nuestras soluciones sean accesibles para todo tipo de clientes; y lograrlo de una manera escalable y basada en estándares”, expresó Chávez. Desde la visión de Persiles Martínez, especialista en Consolidación de Servidores de GBM Corporation, “el concepto de virtualización apunta a separar el

hardware del sistema operativo y las aplicaciones. Esta noción puede ser implementada de múltiples formas, pero fundamentalmente se logra insertando una capa que provee la simulación de las interfaces necesarias entre el componente de *hardware* y el de *software*. De esta manera, se incrementa la utilización de los recursos existentes, además de aumentar los niveles de disponibilidad y de simplificar la estrategia de respaldo-recuperación”, manifestó Martínez.

4.1.5 Herramienta de virtualización a utilizar

Una vez analizado el concepto y las razones de la importancia de la virtualización y de las múltiples ventajas que ésta presenta, es necesario destacar que el ahorro que representa es sólo el comienzo del valor que se ofrece. En la actualidad, la virtualización desempeña un papel significativo para permitir a las empresas crear sistemas de TI que no solo sean muy eficientes, sino que tengan la capacidad de automatizarse y responder de forma eficaz a los cambios que sufren los negocios.

De ahí, que crece la necesidad de poder contar con herramientas tecnológicas que permitan ejecutar con éxito una estrategia de virtualización. Las empresas líderes en este campo aprovechan su saber hacer – para crear productos especializados en esta tecnología, con miras de abarcar la mayor parte del mercado mediante productos y servicios que permiten adaptarse a las necesidades de los negocios así como de sus clientes, brindando computación en tiempo real, más agilidad, mayor continuidad en los negocios y un mejor aprovechamiento de los recursos. Las herramientas de virtualización que actualmente se conocen en el mercado son un gran número.

Acorde al contexto del proyecto a resolver utilizamos el software de virtualización VMware Workstation 10.0. Pues cumple los requisitos de los equipos disponibles para el uso, de igual forma es el software con el que cuenta la Institución.

4.1.6 instalación de VMware Workstation 10.0

Para instalar VMware Workstation hay que seguir los siguientes pasos:

1. Ejecute el archivo .EXE y empezara a preparar la instalación del programa.
2. Pulse en *Next* y le mostrara una pantalla en la que deberá elegir el tipo de instalación que desea realizar (en el ejemplo, *Custom*).
3. Cuando lo baya indicado, pulse en *Next* y pasara a otra pantalla en la que le indica la ubicación donde se va a realizar la instalación (en caso de querer modificarlo, pulse en *Change* y seleccione la nueva ubicación).

-
4. Cuando lo desee, pulse en *Next* y se seleccione los accesos directos que desea colocar (en el ejemplo, se seleccionando los tres indicados).
 5. Cuando haya acabado, pulse en *Next* y, en la nueva pantalla, pulse en *Install* para proceder a instalarlo.
 6. Cuando haya finalizado, le mostrara una pantalla para que indique sus nombre, la empresa y el número de serie (estos datos pueden indicarse posteriormente).
 7. Cuando lo desee, pulse en *Enter* si ha indicado dichos datos o *Skip* si no desea indicarlos en este momento.
 8. Le mostrara la pantalla de finalización del asistente. Pulse en *Finish* y le mostrara una pantalla en la que le indica que debe reiniciar el equipo. Pulse en *Yes* para reiniciarlo.
 9. Cuando se haya reiniciado el equipo, entre a VMware Workstation, acepte la licencia de uso y ya estará completa la instalación.

4.1.7 Creación de una máquina virtual

Una vez que se ha instalado VMware Workstation, se va a proceder a instalar una máquina virtual con Windows 7 en el equipo anfitrión. Para ello, siga los pasos siguientes:

1. Ejecute VMware Workstation del Escritorio o desde el menú Inicio, desmarque en *Show tips at startup* si desea que no vuelva a aparecer la próxima vez que inicie el programa y pulse en *Close* para cerrar dicha ventana.
2. Pulse en *New Virtual Machine* para crear una nueva máquina virtual y vera la ventana siguiente:



Figura 12

3. En ella puede indicar que tipo de configuración desea para la nueva máquina virtual que está creando:

- Typical: Permite crear la máquina virtual de forma rápida y con la configuración estándar.
- Custom: Permite crear la máquina virtual de forma personalizada, pudiendo seleccionar opciones avanzadas, como el tipo de disco virtual y la compatibilidad con productos VMware anteriores.

En este ejemplo usare *Custom* ya que me permite fijar más cosas importantes como el número de núcleos, la memoria, etc., además esta guía está orientada a un uso avanzado de la máquina virtual. Si se elige *Typical* algunos pasos posteriores serán omitidos en la creación de la máquina virtual.

4. En esta ventana se define la versión a la que crearemos la máquina virtual y sus compatibilidades con otros productos VMware así como sus limitaciones. Si trabajaremos con la misma versión en *Hardware compatibility* dejaremos seleccionado “Workstation 6.5-7.0”.



Figura 14



Figura 13

5. En la siguiente pantalla hay tres casillas de verificación:

- Installer disc: Para instalar el sistema operativo invitado desde un CD mientras está creando la máquina virtual.

-
- Installer disc image file (ISO): Para instalar el sistema operativo invitado desde un fichero ISO mientras está creando la máquina virtual (si pulsa en *Browse*, podrá seleccionar el nombre de dicho fichero y la ubicación en la que se encuentra).
 - I will install the operating system later: Para crear la máquina virtual en blanco y, posteriormente, instalar el sistema operativo invitado.



Figura 15

6. En esta ventana indicaremos el nombre con el que deseamos identificar la máquina virtual y su ubicación, para elegir su ubicación utilizaremos el botón *Browse...*



Figura 16

7. Aquí definimos el número de núcleos que queremos que tenga el procesador de nuestra máquina virtual, que si tenemos dos núcleos o más podemos poner hasta cuatro núcleos.

- Number of processors: Numero de procesadores
- Number of cores per processors: Numero de núcleos por procesador

Para el ejemplo utilizaremos un procesador de dos núcleos.

8. En esta ventana especificamos cuanta memoria RAM tendrá el sistema, el triángulo verde nos indica la cantidad recomendada, aunque siempre se puede aumentar según las necesidades.

9. En esta ventana se define el sistema con el que la máquina virtual se conectara a una red.



Figura 17

- **Bridged:** La máquina virtual tendrá su propia IP y creara una conexión puente entre los adaptadores de red del anfitrión y el invitado, permitiendo la conexión a red de ambos a través del adaptador del anfitrión.

- **NAT:** La IP de la máquina virtual ser dinámica y utilizara el sistema anfitrión como proxy en las conexiones de red.

- **Host only:** Seria como conectar un cable cruzado entre anfitrión e invitado y se podría compartir archivos entre ellos, la IP seria dinámica.

- **Do not use a network connection:** Sin conexión de red.

10. Aquí definimos el adaptador para los dispositivos de E/S principalmente para los SCSI, dejamos la opción recomendada: *LSI Logic SAS*.



Figura 18

11. Aquí decidimos que disco usaremos en la máquina virtual:

- Create a new virtual disk: Se crearan uno o varios archivos en la maquina anfitrión aunque en la maquina invitada aparecerá como uno solo. Los discos virtuales pueden ser copiados o movidos fácilmente en el mismo equipo o entre varios.
- Use an existing virtual disk: Para usar un disco virtual ya creado previamente.
- Use a physical hard disk: La máquina virtual tendrá acceso directo a un disco duro del equipo.

12. En esta ventana definimos el tipo de disco duro que tenemos conectado en la máquina virtual. La opción recomendada es SCSI.

13. En la siguiente pantalla deberá detallar cómo será el disco duro virtual:



Figura 19



Figura 20

- Maximum disk size: Tamaño máximo del disco duro.
- Allocate all space disk now: Esta opción reservara todo el espacio requerido por el disco virtual, solo es recomendable si se dispone de mucho espacio ya que aumenta algo el rendimiento. Dejándola desmarcada depende de cuánto metamos en el disco duro virtual el archivo ocupara más o menos.
- Store virtual disc as a single file: Para guardarlo como un único archivo.
- Split virtual disc into 2 GB files:) Para dividirlo en trozos de 2Gb cada uno. Esta opción se utiliza si se va a copiar el archivo para llevarlo de una maquina a otra o se tiene formateada la partición/disco en FAT-16 o FAT-32.

Como norma general se deja el valor por defecto ya que es el recomendado y las otras opciones se elige según el sistema de archivos (FAT/NTFS).



Figura 19

14. En esta ventana nos deja la puerta abierta para cambiar la ubicación del disco duro respecto a los demás archivos que componen la máquina virtual, aunque no se suele cambiar.

Una aplicación práctica de esta opción sería poder ubicar el disco duro virtual en una segunda partición menos usada con más espacio libre ya que de todos los archivos que componen la máquina virtual el disco duro virtual es el elemento que más ocupa (varios gigas después de un instalación completa).

15. En esta ventana se mostrara un resumen de la configuración que hemos especificado en los pasos anteriores. Si quieres modificarla, pulsa en *Customize hardware* para modificar la máquina virtual, sino pulsa en *Finish* para proceder a su creación.

4.1.8 Instalación de sistema operativo en una máquina virtual

La máquina que se virtualizara tendrá que usar el sistema operativo que se utiliza en la cruz roja mexicana el cual es Windows XP para poder hacer las pruebas pertinentes de manera idéntica como con una maquina física.

Una vez que se ha creado la máquina virtual, para instalar un sistema operativo siga los pasos siguientes:

1. Ejecute VMware Workstation desde el escritorio o el Menú Inicio.
2. Sitúese en *Favorites* (se encuentra en el panel izquierdo), en caso de que no esté visible dicho panel, pulse en el icono *Show or hide Sidebar* que se encuentra en el octavo lugar empezando por la izquierda) sobre la máquina virtual que desee y, en el panel derecho, pulse en *Edit virtual machine settings*.

3. En la ficha *Hardware*, seleccione CD/DVD (IDE) e indique de qué forma quiere cargar el disco de instalación. Ya sea por unidad física (*Use Physical Drive*) o con una imagen ISO (*Use ISO image file*).



Figura 20

4. Guarde la nueva configuración de la máquina virtual.

5. Estando situado en la máquina virtual, seleccione *Power on this virtual machine* y empezara a ejecutarla.

6. Comenzará la instalación del sistema operativo exactamente igual que con la maquina física.

Tenga en cuenta que si no pulsa sobre la máquina virtual o [Ctrl]+[G] no se podrá actuar sobre ella, para volver al sistema anfitrión, deberá pulsar [Ctrl]+[Alt].

7. Cuando haya finalizado la instalación apague el sistema operativo y cierre la aplicación.

Es recomendable apagar el sistema operativo siguiendo el procedimiento de este, aunque en última instancia también se puede apagar pulsando en el icono *Power Off* que se encuentra en el primer lugar empezando por la izquierda, pero no es recomendable, ya que el sistema operativo no se habrá cerrado correctamente.

16. Una vez finalizada la creación deberá ver lo siguiente:

- En el panel izquierdo, el nombre de la máquina virtual en *Favorites*
- En el panel derecho, la configuración de la máquina virtual. Desde aquí se puede modificar dicha configuración o ejecutar la máquina virtual. Ambas cosas se describirán en apartados posteriores.

4.1.9 Ejecución de la máquina virtual

Una vez instalado el sistema operativo en la máquina virtual, para ejecutarlo con VMware Workstation siga los pasos siguientes:

1. Ejecute VMware Workstation desde el escritorio o el Menú inicio.
2. Sitúese en *Favorites* (se encuentra en el panel izquierdo), en caso de que no esté visible dicho panel, pulse en el icono *Show or hide Sidebar* que se encuentra en el octavo lugar empezando por la izquierda) sobre la máquina virtual que desee y, en el panel derecho, pulse en *Power on this virtual machine* y empezara a ejecutarla. Es posible que durante la carga de la máquina virtual, le aparezca un mensaje en el que le indica los dispositivos removibles que pueden conectarse, cuando lo haya leído, pulse en OK.
3. Cuando finalice la carga del sistema e iniciada la sesión, vaya al Administrador de dispositivos de la máquina virtual (se encuentra en la ficha *Hardware* de “Propiedades” del menú contextual de Mi PC), para ver si hay dispositivos que están deshabilitados. Cuando haya terminado, cierre todas las pantallas y vuelva al Escritorio.
4. Pulse en el icono *Summary View* (se encuentra en el quinto lugar empezando por la derecha), sitúese en *Network Adapter* de la ficha *Devices* y vea en qué modo esta (Bridged, NAT o Host-only).

En el sistema operativo invitado (deberá pulsar en el icono *Console View* que es el tercero empezando por la derecha), vaya a “Conexión de área local” (se encuentra en “Propiedades” del menú contextual de “Mis sitios de red”), muestre su menú contextual, seleccione “Propiedades”, sitúese sobre “Protocolo de Internet (TCP/IP)”, pulse en “Propiedades” y vea el direccionamiento IP que tiene. Recuerde:



Figura 21

-
- Si esta en modo Bridged y no dispone de servidor DHCP en la red, deberá indicar una dirección IP estática para la máquina virtual en el mismo rango que el equipo anfitrión y si desea tener acceso a Internet, deberá indicar la dirección IP de la puerta de enlace y de los servidores DNS.
 - Si esta en modo Host-only, el direccionamiento IP de la máquina virtual ha de ser difundido y VMware le adjudicará una dirección IP.
 - Si esta en modo NAT, el direccionamiento IP de la máquina virtual ha de ser dinámico y VMware le adjudicará una dirección IP. Además, le añadirá una puerta de enlace virtual y utilizará el anfitrión como proxy.

5. Si conecta un nuevo dispositivo USB en la máquina virtual observe en la parte derecha de la barra de tareas que lo ha reconocido. Si es la primera vez, el sistema tendrá que instalar controladores tanto en el sistema anfitrión como en el invitado, sino solo habrá que hacerlo en el invitado.

6. Si desea tomar una instantánea, pulse en el icono *Take Snapshot of Virtual Machine* (se encuentra en el quinto lugar empezando por la izquierda), indique el nombre que desea dar a la instantánea, una breve descripción, pulse en OK y comenzará a realizarla (otra alternativa es desde el menú VM, seleccionar *Snapshot* y, después, *Take Snapshot*).

Ahora puede seguir trabajando y haciendo las pruebas que desee con el sistema operativo invitado. Cuando desee volver al estado en el que se encontraba cuando realizó la instantánea anterior, pulse en el icono *Revert Virtual Machine to Snapshot <Nombre>* (se encuentra en el sexto lugar empezando por la izquierda) y el sistema operativo se reiniciará en el estado anterior.

Si desea ver las instantáneas que hay establecidas, pulse en el icono *Manage Snapshots for Virtual Machine* (se encuentra en el séptimo lugar empezando por la izquierda). Desde allí, puede borrar la que desee, seleccionándola y pulsando en *Delete* (deberá confirmar el borrado). Cuando haya finalizado, pulse en *Close* para salir de dicho administrador (otra alternativa es desde el menú VM, seleccionar *Snapshot* y, después, *Snapshot Manager*).

7. Grabaciones. Otra posibilidad de la que dispone es grabar las operaciones que realice con la máquina virtual. Para ello, pulse en el icono *Record Execution of Virtual Machine* (se encuentra en el segundo lugar empezando por la derecha) y comenzaría a realizar una instantánea del estado en el que se encontraba la máquina en ese momento. Después, le mostrará en la parte superior izquierda una ventana en la que puede ver que se está grabando (es posible que le muestre algún mensaje de aviso anteriormente. Pulse en OK para continuar, todo lo que realice, se grabará hasta que pulse en el icono en forma de cuadrado azul que se encuentra en dicha ventana. Entonces, se parará la grabación y le pedirá que indique un nombre para la grabación. Cuando lo haya realizado, pulse en *Save* y se guardará.

Cuando quiera ver dicha grabación, pulse en el icono *Replay* <nombre> (se encuentra en el primer lugar empezando por la derecha) y comenzara a ver la grabación. (Es posible que le muestre algún mensaje de aviso anteriormente. Pulse en OK para continuar.

8. Si desea capturar una pantalla y cogerla desde el sistema operativo anfitrión, abra el menú VM, seleccione *Capture Screen* y la pantalla se guardara en el portapapeles. Cuando lo desee, seleccione *Pegar* y se pasara a la aplicación que esté utilizando.

9. Si desea utilizar carpetas compartidas con el anfitrión, deberá instalar las VMware Tools.

10. Cuando haya finalizado, ya puede proceder a utilizar la máquina virtual para trabajar con el sistema operativo invitado.

11. Cuando le parezca, apague el sistema operativo y cierre la máquina virtual (puede cerrar la máquina virtual pulsando en el icono *Power off of Virtual Machine* que se encuentra en el primer lugar empezando por la izquierda, pero no es recomendable, ya que el sistema operativo no se habrá cerrado correctamente.

4.1.10 Instalación de Ipv6 en Windows XP

Para instalar IPv6 en el equipo con Windows XP, siga estos pasos:

Haga clic en Inicio, seleccione Todos los programas, Accesorios y, a continuación, haga clic en símbolo del sistema.

En el símbolo del sistema, escriba *netsh int ipv6 install* y presione la tecla Intro en el teclado.

Cierre la ventana de símbolo del sistema.

4.2 Configuración del router

Como hemos mencionado anteriormente tendremos que configurar el router de cisco para que la red hibrida pueda funcionar adecuadamente.

Por lo tanto tendremos que configurar un túnel de salida a internet con 6to4, también 6pe para trabajo de intranet nativa en ipv6 y mantener el servicio de ipv4 para la intranet con NAT64 y DNS 64.

4.2.1 Configuración de router cisco para 6to4

Ahora configuramos el router para crear un túnel 6to4 que es el mecanismo de encapsulamiento en ipv4 con datos internos en ipv6. Este lo utilizaremos para la conexión a internet.

Entramos al modo consola del router y a continuación se menciona la configuración.

Tabla 2

```
router# configure terminal
router(config)# ipv6 unicast-routing
router(config)# interface Tunnel2002
router(config-if)# no ip address
router(config-if)# no ip redirects
router(config-if)# ipv6 address 2002:A750:81D2::1/128
router(config-if)# tunnel source FastEthernet
```

4.2.2 Configuración de 6pe

Utilizamos 6pe para crear una intranet nativa en ipv6 ejecutando el modo consola en el router cisco y a continuación se muestra la configuración de 6pe:

```
Mpls ipv6 source interface loopback0
```

```
Router bgp numero ASN
```

```
Address-family ipv6
```

```
Redistribute connected route-map accion-conectadas
```

```
Redistribute static route-map accion-estaticas
```

```
Neighbor direction-IP-RR active
```

```
Neighbor direction-IP-RR send-community
```

```
Neighbor direction-IP-RR send label
```

```
Neighbor direction-IP-RR peer-group nombre-grupo
```

```
Exit-address-family
```

4.2.3 Configuración de nat 64

Como se mencionó anteriormente tenemos que utilizar NAT64 conservar el acceso al servicio Internet IPv4 para la Intranet. Se coloca la configuración de router a continuación:

```
Router> enable

Router# configure terminal

Router(config)# ipv6 unicast-routing

Router(config)# interface giabitethernet0/0/0

Router(config-if)# description interface towards ipv4 side

Router(config-if)# ipv6 enable

Router(config-if)# ipv6 address 2001:1::/96

Router(config-if)# nat64 enable

Router(config-if)# exit

Router(config)# interface giabitethernet1/2/0

Router(config-if)# description interface towards ipv6 side

Router(config-if)# ip address 192.168.0.0 255.255.255.0

Router(config-if)# nat64 enable

Router(config-if)# exit

Router(config)# nat64 prefix stateless 2001:0db8:0:1::/9

Router(config)# nat64 route 192.168.0.0/24 gigabitethernet0/0/1

Router (config) # end
```

4.2.4 Implementación de un dns64

El mecanismo NAT64 funciona por medio de un servidor DNS64 que recibe las consultas de clientes IPv6, el servidor DNS64 a su vez se comunica con otros servidores DNS (Albitz& Liu, 2006) ubicados en Internet. Cuando la consulta corresponde a un nombre de host que tiene dirección IPv4, el DNS64 transforma esta dirección en una dirección IPv6 anteponiéndole el prefijo que identifica el servicio NAT64. La red debe estar configurada de tal forma que los paquetes enviados a un destino que contenga el prefijo del NAT64, utilicen el encaminador NAT64 como puerta de enlace, la función de este encaminador es convertir paquetes IPv6 en paquetes IPv4 y viceversa.

Para que lo anteriormente mencionado se cumpla vamos a utilizar Bind para en un servidor DNS sobre Windows xp.

4.2.4.1 Implementación de Bind en Windows XP:

Ejecutar el instalador

Esto va a instalar el Bind y todas sus aplicaciones en el directorio `\Windows\system32\dns\`.

Dejamos la opción Automatic Startup

Dentro del directorio de instalación hay dos carpetas llamadas bin y etc.

Vamos a Inicio Ejecutar y escribimos "cmd" y damos enter.

En el cursor escribimos "cd \Windows\system32\dns\bin\" y damos enter.

Con esto estamos dentro de la carpeta bind.

Ahora tecleamos "rndc-confgen > rndc.conf" y de nuevo enter.

Este comando crea un archivo llamado rndc.conf que tenemos que copiar a la otra carpeta o sea "etc".

Entonces abrimos MI PC y vamos hasta `\Windows\system32\dns\bin\` y en el archivo rndc.conf le hacemos clic derecho y copiar.

Subimos un nivel y vamos a la carpeta \etc. y pegamos el archivo.

Ya que estamos dentro de la carpeta etc. creamos dos archivos de texto con el bloc de notas y le ponemos como nombre a uno resolv.conf y al otro named.conf.

Editar el archivo resolv.conf y escribimos esta línea "nameserver 127.0.0.1"

En este archivo se anotan los DNS y 127.0.0.1 es un IP reservada (no se ve desde Internet) que se llama local host, es la IP que usa nuestra máquina para comunicarse con sí misma.

Descargar ftp://ftp.rs.internic.net/domain/named.root y ese archivo named.root también lo copiamos a etc.

Vamos a Panel de Control/ Conexiones de red y buscamos la que tenemos activa, le damos clic derecho y Propiedades, marcamos Protocolo Internet TCP-IP y damos clic a el botón propiedades, donde dice DNS preferido se borra el número de IP y escribimos 127.0.0.1

Damos clic en Guardar.

4.2.4.2 Activar el funcionamiento de DNS64 en BIND

Se debe adicionar al archivo de opciones del servidor BIND. Para activar el funcionamiento del router NAT64, basta con descargar el disco compacto “cd-live” que se encuentra disponible en Viagénie (2010), configurar las direcciones IPv4 e IPv6 sobre las interfaces de la estación y ejecutar el script de configuración “nat64-config.exe” que se encuentra dentro del “cd-live”.

4.3 Pruebas virtualizadas

Para iniciar las pruebas se virtualizo un equipo en Windows XP service pack 3 y un servidor DNS de BIND en Windows XP service pack 3, conectando a los routers de cisco previamente configurados con 6to4, NAT 64 y IPV6, mediante un cuarto router con ipv6.

4.3.1 Prueba 6to4

Se muestra en la parte de abajo una estación Windows XP service pack 3, ubicada dentro de la red IPv6 nativa, probando que existe conexión entre la red IPv6 nativa y la Internet IPv6 representada por la dirección IPv6 global 2000:1000:100::1/64. Como se puede observar en la figura.

Tabla 3

```
C: /Users/Sistemas2 ping 9.19.99.36
haciendo ping a 9.19.99.36 con 32 bytes de datos
respuesta desde 9.19.99.36 bytes=32 tiempo 42ms TTL=47
respuesta desde 9.19.99.36 bytes=32 tiempo 42ms TTL=47
respuesta desde 9.19.99.36 bytes=32 tiempo 42ms TTL=47
respuesta desde 9.19.99.36 bytes=32 tiempo 42ms TTL=47

Estadísticas de ping 9.19.99.36
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    <=%perdidos>
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 41ms, Máximo = 42ms, Media =
    41ms
```

4.3.2 Prueba Nat64

Las líneas 1 a 4 de la figura presentan una captura para verificar el funcionamiento de este mecanismo. En la figura 8 se puede observar la interrogación desde la estación IPv6 de la red IPv6 nativa de la oficina central hacia el servidor de aplicación IPv4 (9.19.99.227) ubicado.

Las líneas 5 a 8 y 9 a 12 de la figura presentan una captura realizada con el analizador de protocolos Wireshark (Combs, 1998) sobre las dos interfaces de “R. NAT64”. Al relacionar la figura, se puede deducir que el router recibe los paquetes IPv6 en su interfaz conectada a la red IPv6 nativa, convierte los paquetes IPv6 en paquetes IPv4, y envía dichos paquetes IPv4 hacia su respectivo destino, usando su interfaz conectada a la red Internet IPv4. En el sentido contrario se presenta el proceso opuesto en la traducción de los paquetes IP.

Tabla 4

<ol style="list-style-type: none">1. Sistemas2 ping6 Servidor Expediente2. haciendo ping a 9.19.99.210 con 32 bytes de datos respuesta desde 9.19.99.210 bytes=32 tiempo 42ms TTL=47 respuesta desde 9.19.99.210 bytes=32 tiempo 42ms TTL=47 respuesta desde 9.19.99.210 bytes=32 tiempo 42ms TTL=47 respuesta desde 9.19.99.210 bytes=32 tiempo 42ms TTL=473. Ethernet II, Src: CadmusCo_94:c2:1e (08:00:27:94:c2:1e), Dst: c2:00:0d:d4:00:00 (c2:00:0d:d4:00:00)4. Internet protocol version 6, Src: 2002:c010:101:64::20 (2002:c010:101:64::20), Dst: 64:ff9b::c214:114 (64:ff9b::c214:114)5. Internet Control Message Protocol v66. Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)7. Ethernet II, Src: CadmusCo_14:67:f0 (08:00:27:14:67:f0), Dst: c2:01:0d:d4:00:00 (c2:01:0d:d4:00:00)8. Internet protocol, Src: 192.16.4.64 (192.16.4.64), Dst: 194.20.1.20 (194.20.1.20)9. Internet Control Message Protocol
--

4.3.3 Prueba de cliente servidor

Para validar el funcionamiento correcto del mecanismo NAT64 se estableció una conexión entre una estación IPv6 nativa (ejecutando un programa cliente de navegación) y un servidor Web IPv4 (9.19.99.36) Se logró evidenciar que la estación IPv6 se pudo conectar al servidor del Expediente IPv4 (9.19.99.210), a través del NAT64, este último equipo es el encargado de traducir la dirección IPv6 (64:ff9b::C9E8:7B09) a su correspondiente dirección IPv4 (9.19.99.210)y, finalmente enviar la respectiva respuesta a la estación cliente. En la prueba realizada se pudo probar que la capa de aplicación no se afectó por la traducción NAT64.

4.4 Implementación física

Dado que las pruebas en equipos virtualizados fueron exitosas se procedió a implementar la ipv6 en 10 equipos de Windows xp service pack 3, puesto que no se puede llevar a cabo la implementación total de este proyecto por motivos económicos de la institución.

Se dio de alta la función de ipv6 en los equipos y se conectaron al mismo router de los equipos virtualizados.

Cabe señalar que el servidor DNS que fue virtualizado será el mismo que se dejó implementado.

Se llevaran a cabo las mismas pruebas que en las máquinas virtuales.

4.4.1. Pruebas físicas

Para iniciar las pruebas se usaron los equipos Windows XP service pack 3 y el servidor DNS de BIND en Windows XP service pack 3 virtualizado, conectando a los routers de cisco previamente configurados con 6to4, NAT 64 y IPV6, mediante un cuarto router con ipv6.

4.4.2 Prueba 6to4 (física)

Se muestra en la parte de abajo una estación Windows XP service pack 3, ubicada dentro de la red IPv6 nativa, probando que existe conexión entre la red IPv6 nativa y la Internet IPv6 representada por la dirección IPv6 global 2000:1000:100::1/64. Como se puede observar en la figura.

Tabla 5

<pre>C: /Users/Sistemas2 ping 9.19.99.100 haciendo ping a 9.19.99.100 con 32 bytes de datos respuesta desde 9.19.99.100 bytes=32 tiempo 42ms TTL=47 respuesta desde 9.19.99.100 bytes=32 tiempo 42ms TTL=47 respuesta desde 9.19.99.100 bytes=32 tiempo 42ms TTL=47 respuesta desde 9.19.99.100 bytes=32 tiempo 42ms TTL=47</pre>

4.4.3 Prueba Nat64 (física)

Las líneas 1 a 4 de la figura presentan una captura para verificar el funcionamiento de este mecanismo. En la figura 8 se puede observar la interrogación desde la estación IPv6 de la red IPv6 nativa de la oficina central hacia el servidor de aplicación IPv4 (9.19.99.227) ubicado.

Las líneas 5 a 8 y 9 a 12 de la figura presentan una captura realizada con el analizador de protocolos Wireshark (Combs, 1998) sobre las dos interfaces de "R. NAT64". Al relacionar la figura, se puede deducir que el router recibe los paquetes IPv6 en su interfaz conectada a la red IPv6 nativa, convierte los paquetes IPv6 en paquetes IPv4, y envía dichos paquetes IPv4 hacia su respectivo destino, usando su interfaz conectada a la red Internet IPv4. En el sentido contrario se presenta el proceso opuesto en la traducción de los paquetes IP.

Tabla 6

- | |
|--|
| <ol style="list-style-type: none">1. Sistemas2 ping6 Servidor Expediente2. haciendo ping a 9.19.99.227 con 32 bytes de datos
respuesta desde 9.19.99.227 bytes=32 tiempo 42ms TTL=47
respuesta desde 9.19.99.227 bytes=32 tiempo 42ms TTL=47
respuesta desde 9.19.99.227 bytes=32 tiempo 42ms TTL=47
respuesta desde 9.19.99.227 bytes=32 tiempo 42ms TTL=473. Ethernet II, Src: CadmusCo_94:c2:1e (08:00:27:94:c2:1e), Dst: c2:00:0d:d4:00:00 (c2:00:0d:d4:00:00)4. Internet protocol version 6, Src: 2002:c010:101:64::20 (2002:c010:101:64::20), Dst: 64:ff9b::c214:114 (64:ff9b::c214:114)5. Internet Control Message Protocol v66. Frame 8: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)7. Ethernet II, Src: CadmusCo_14:67:f0 (08:00:27:14:67:f0), Dst: c2:01:0d:d4:00:00 (c2:01:0d:d4:00:00)8. Internet protocol, Src: 192.16.4.64 (192.16.4.64), Dst: 194.20.1.20 (194.20.1.20)9. Internet Control Message Protocol |
|--|

4.4.4 Prueba de cliente servidor

Para validar el funcionamiento correcto del mecanismo NAT64 se estableció una conexión entre una estación IPv6 nativa (ejecutando un programa cliente de navegación) y un servidor Web IPv4 (9.19.99.36) Se logró evidenciar que la estación IPv6 se pudo conectar al servidor del Expediente IPv4 (9.19.99.227), a través del NAT64, este último equipo es el encargado de traducir la dirección IPv6 (64:ff9b::C9E8:7B09) a su correspondiente dirección IPv4 (9.19.99.227)y, finalmente enviar la respectiva respuesta a la estación cliente. En la prueba realizada se pudo probar que la capa de aplicación no se afectó por la traducción NAT64.

Conclusiones

La transición hacia IPv6 es un paso que las entidades se ven obligadas a realizar en el corto plazo debido al rápido agotamiento de las direcciones IPv4, esto se debe llevar a cabo de una manera planeada y sistemática, minimizando el impacto en la operación de la red.

Una aproximación que demanda menor administración de recursos de procesamiento, se basa en un modelo en el que se implementa una red IPv6 nativa en la oficina central, teniendo conectividad IPv6 con las oficinas remotas mediante 6PE, y acceso a la Internet IPv6 mediante 6to4. El uso de DNS64, combinado con el reciente mecanismo de traducción NAT64, hace posible implementar IPv6 de forma nativa sin perder el acceso a los servicios que se presten en la Internet IPv4. Dos opciones que se pueden usar cuando el ISP no soporte 6to4, son el mecanismo Tunnel Broker o el mecanismo 6rd; estas realizan la misma función de 6to4 y facilitan la depuración de la conexión. La integración de GNS3 con estaciones virtuales es una herramienta que les permite a las empresas crear laboratorios de pruebas completos dentro de una sola máquina y validar cada uno de los pasos en el proceso de migración hacia IPv6.

Como se ha demostrado nuestra hipótesis fue demostrada en operaciones habituales de un administrador de red. Y son esto no solo ayudara a las operaciones diarias de la institución si no al crecimiento de la una red más estable y rápida. Y a la certificación de los estándares de servicios que aporta la CRUZ ROJA MEXICANA DELEGACIÓN DISTRITO FEDERAL.

Bibliografía.

Cisco Systems Inc. (2002). *IPv6 over MPLS (Cisco 6PE)*.

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/iosip_an.pdf

Cisco Systems Inc. (2008). *Cisco IOS IPv6 configuration Guide*.

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/12_4/ipv6_12_4_book.pdf

Combs, G. (1998). *Wireshark*. <http://www.wireshark.org>

Deering, S., & Hinden, R. (1998). *Internet Protocol, Version 6 (IPv6) Specification*. In IETF (The Internet Engineering Task Force)

Request for Comments 2460. <http://www.ietf.org/rfc/rfc2460.txt>

Dooley, K., & Brown, I. (2006). *Cisco IOS CookBook*. Sebastopol, California: O'Reilly Media, Inc.

Frankel, S., Graveman, R., Pearce, J., & Rooks, M. (2010). *Guidelines for the Secure Deployment of IPv6*. National Institute of Standards and Technology.

<http://www.nist.gov/publications/nistpubs/800-119/sp800-119.pdf>

Grossmann, J., Marsili, B., Goudjil, C., Thamini, X., & Eromenko, A. (2008). *GNS3: Graphical Network Simulator Software*. <http://www.gns3.net>.

<http://portalipv6.lacnic.net/es/quienes-est-n-implementando-ipv6-en-la-regi-n> visitado el 4 de enero de 2013 a las 10:43 hrs

<http://www.internetsociety.org/businesses-and-industries-short-guide-ipv6/> visitado 4 de enero 2013 a las 12:03 hrs

http://es.wikipedia.org/wiki/Red_de_computadoras visitada el 7 de enero de 2013 a las 13:17 hrs

<http://www.dgis.salud.gob.mx/normatividad/nom024.html> visitada el 8 de enero del 2013 a las 16:15 hrs

<http://gobiernoti.wordpress.com/2011/10/04/tipos-de-redes-informaticas/> visitado el 22 de marzo del 2013 a las 19:32 hrs.

<http://www.monografias.com/trabajos40/redes-informaticas/redes-informaticas2.shtml#concl> visitado el 19 de mayo del 2013 a las 16:50

<http://gigatecno.blogspot.mx/2012/03/ventajas-y-desventajas-de-las-redes.html> visitado el 21 de mayo del 2013 a las 19:30

<http://www.dgjs.salud.gob.mx/normatividad/nom024.html> visitado el 28 de mayo del 2013 a las 22:30

http://www.financialtech-mag.com/docum/138_DocumentoC_2.pdf consultado el 22 de noviembre de 2013 a las 7:58 a.m