FACULTAD DE INGENIERÍA Y CIENCIAS AGROPECUARIAS

DISEÑO DE LA ESTRATEGIA DE MIGRACIÓN TÉCNICA DE LA INFRAESTRUCTURA IPv4 A UNA INFRAESTRUCTURA IPv6 EN EL AREA DE NETWORKING DE LA SECRETARIA DE HIDROCARBUROS DE ECUADOR

Trabajo de Titulación presentado en conformidad con los requisitos establecidos para optar el Título de Ingeniero en Redes y Telecomunicaciones

Profesor guía
Ing. Mario Andrés Jaramillo Astudillo

Autor
Héctor Xavier Toapanta Oyos

Año
2014

DECLARACIÓN PROFESOR GUÍA

Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación.

_____

Mario Andrés Jaramillo Astudillo
Ingeniero Electrónico
C.I. 0102424207

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.

_____

Héctor Xavier Toapanta Oyos

1714142559

RESUMEN

La presente tesis fue realizado en base a una necesidad tecnológica que se presentará a futuro como lo es la tecnología IPv6, también conocida como el Internet de las cosas, en base a esto se planteó realizar un análisis en la infraestructura tecnológica de la Secretaría de Hidrocarburos.

Como preámbulo al análisis de un sistema de comunicaciones se debe tomar en cuenta el estudio del modelo OSI como un estándar de las telecomunicaciones, adicionalmente se revisa las características, composición, direccionamiento y usos de los protocolos IPv4 e IPv6.

Posteriormente se describe la situación actual de la red LAN y WAN de la entidad, tomando como referencia el direccionamiento que posee, configuración de VLANs, direccionamiento y servicios que actualmente posee.

Se considera las diferentes técnicas que existe para realizar la migración de un protocolo IPv4 a un protocolo IPv6, tomando en cuenta a la forma nativa IPv6, es decir que todo el direccionamiento de la red sea IPv6, túneles manuales, túneles automáticos que existe para transportar paquetes desde una red IPv6 a través de una red IPv4 de un proveedor de servicios de Internet con destino en una red IPv6, adicionalmente se recomienda el direccionamiento IPv6 a utilizar y los cambios de configuraciones que se deben ejecutar en equipos servidores y clientes.

Una vez revisadas las diferentes técnicas de migración se procede a realizar con software de simulación PacketTracert de Cisco, tanto en la red LAN y WAN, en lo referente a los equipos servidores se realiza una configuración de los ámbitos de DHCP que se deberán crear.

Finalmente se concluye y recomienda acerca de las consideraciones a tomar en cuenta en el proceso de migración.

ABSTRACT

The following thesis was made based on a technological need that will become in the future, as the IPv6 technology, also known as the things internet, in regard of this, I established to analyze the “Secretaría de Hidrocarburos” technological infrastructure.

As preamble of the communications systems analysis, we have to consider the OSI model study as a telecommunications standard, besides we have to check the IPv4 and IPv6 forms characteristics, composition, course and uses.

Afterwards, I describe the LAN and WAN entity actual net situation, considering as reference the course, VLANs configuration, services and course it actually has.

It is considered the different techniques we have to do for the IPv4 form migration to a IPv6 form, considering the native form IPv6; every net course will have to be IPv6, manual tunnels, automatic tunnels to transport packets from an IPv6 net through an IPv4 net from an internet services supplier with destination to an IPv6 net, also I recommend the IPv6 course to use and the configuration changes to use on server equipments and clients.

Once the different migration techniques were checked, we have to make the Cisco PacketTracert software simulation, on WAN and LAN net; relating to server equipments we have to make a DHCP ambits configuration to be created.

Finally, I conclude and recommend about the considerations to notice on the migration process.

ÍNDICE

INTRODUCCIÓN

Antecedentes

Actualmente las redes LAN y WAN usan como protocolo de la capa de redIPv4, este funciona mediante la asignación de un único número a cada uno de los que equipos que quieran acceder a los servicios que ofrece una red.

Las características más importantes de este protocolo son:

- No establece conexión antes de enviar los datos.
- No usan encabezados para garantizar la entrega de paquetes, conocido también como máximo esfuerzo.
- Funciona sin importar los medios que lo transportan.
- Es un protocolo de 32 bits.
- El número máximo de direcciones IP alcanza los 4, 294, 967,295.

A nivel WAN, la administración y asignación de direcciones IPv4 lo realizan las empresas que proveen los servicios de comunicación de datos e Internet.

Debido al crecimiento de la Internet, estas direcciones han disminuido en el mundo, razón por la cual se establece la necesidad de desarrollar un protocolo que permita incrementar el número de direcciones IP.

Haciendo referencia a los antecedentes mencionados se hace posible que se establezca un nuevo protocolo de comunicaciones denominado IPv6.

En algunos sitios de internet se puede verificar que responden con direcciones IPv6, este protocolo nos permite tener 670 mil billones de direcciones IPs, por lo tanto, siendo necesario que las empresas que acceden a la Internet realicen análisis o diseñen estrategias técnicas que permitan migrar a este nuevo direccionamiento.

Entre las características del protocolo IPv6 podemos indicar las siguientes:

- Es un protocolo de 128 bits.
- Permite obtener billones de direcciones IP.
- Soporta IPSEC considerándolo como nativo.
- La comunicación es punto a punto, no necesita NAT para navegar en internet.
- Es auto configurable.
- El encabezado es simple, por lo tanto no tiene checksum, broadcast.
- Es eficiente al momento de realizar enrutamiento.
- Permite compatibilidad con equipos móviles.

En lo referente a la tecnología de direccionamiento que actualmente tiene la Secretaria de Hidrocarburos, se basa en el protocolo IPv4 administrado mediante un sistema Active Directory con el servicio de DHCP habilitado, este asigna de forma automática las direcciones IP, adicionalmente se utiliza VLAN en sus equipos de comunicaciones, manejando el tráfico de voz, video y datos de forma ordenada.

La Secretaria de Hidrocarburos es una entidad que fue creada en Julio del 2010, encargándose de ejecutar actividades de suscripción, modificación y administración de áreas y contratos petroleros, así como los recursos hidrocarburíferos del país.

Actualmente se encuentra domiciliada en la ciudad de Quito, en la Av. Amazonas N35-89 y Juan Pablo Sanz, Edif. Amazonas 4000.

Alcance

El alcance de este trabajo de titulación fue diseñar la estrategia de migración técnica de la infraestructura IPv4 a una infraestructura IPv6 para lo cual se analizó la infraestructura actual y los parámetros utilizados en la red LAN y WAN de la Secretaria de Hidrocarburos de Ecuador.

Se investigará el direccionamiento propuesto para la migración al protocolo IPv6 y se diseñará la estrategia técnica de migración efectuando el análisis con herramientas de software como Packet Tracert y GNS3, estos permite realizar simulaciones de equipos de telecomunicaciones como routers, switch, etc. Para la evaluación de sistemas operativos tipo servidor se utilizó software de virtualización como virtual box de Oracle y Hyper V de Microsoft.

Para el cumplimiento de lo planteado se analizó los diferentes protocolos utilizados en el transporte de datos a nivel LAN y WAN.

Se documentó los procesos necesarios para la migración de la infraestructura actual hacia una infraestructura basada en IPV6.

Se implementó un escenario de pruebas para validar la solución propuesta y para finalizar se realizará un análisis económico del mismo.

La solución propuesta se la pone de manifiesto a la Secretaria de Hidrocarburos para su análisis y de ser el caso su posterior implementación.
Se tomó en cuenta lo aprendido en las materias:

- Interedes locales.
- Conectividad WAN.
- Redes multiservicio.
- Certificación de redes.
- Administración de redes.
- Aplicaciones y servicios convergentes.

Justificación

El continuo desarrollo de la tecnología y la demanda masiva de acceso a Internet en el mundo nos ha llevado a que el direccionamiento a través del protocolo IPV4 sea cada vez más escaso, razón por la cual se debe buscar un

mecanismo que permita utilizar un protocolo que maneje un direccionamiento IP más extenso.

Para el caso de este estudio se plantea un análisis técnico que nos permita migrar hacia el protocolo IPV6. Es posible indicar que en el Acuerdo-No.-039-2012 del Ministerio de Telecomunicaciones de Ecuador, consideran como política del estado ecuatoriano, para las entidades públicas y privadas, realizar los análisis necesarios para interactuar con el protocolo IPV6 tanto a nivel LAN como WAN.

Objetivo General

Diseñar una estrategia de migración técnica que permita realizar el cambio de una infraestructura IPv4 a una infraestructura IPv6 en el área de networking de la Secretaría de Hidrocarburos de Ecuador.

Objetivos específicos

- Analizar la infraestructura actual que posee la Secretaria de Hidrocarburos.
- Analizar los parámetros utilizados en la red LAN de la Secretaria de Hidrocarburos.
- Analizar los parámetros utilizados en la red WAN de la Secretaria de Hidrocarburos que permite conectividad con empresas proveedoras de Internet y enlace de datos.
- Analizar el direccionamiento propuesto para la migración al protocolo IPv6.
- Diseñar la estrategia técnica de migración propuesta para la migración técnica del protocolo IPv4 a IPv6 de la Secretaria de Hidrocarburos.
- Implementar un escenario de pruebas de la solución propuesta.
- Realizar un análisis económico de la propuesta de migración.

1. Marco teórico

1.1 Modelo OSI

Actualmente el desarrollo de la tecnología ha hecho que la sociedad utilice los diferentes servicios que ofrece la Internet, entre las más utilizadas se destacan aplicaciones donde se puede enviar y recibir información como el correo electrónico, mensaje de texto, transacciones en línea, comercio electrónico.

En la figura 1, se muestra las siete capas del modelo OSI y que posteriormente se explicará cómo interactúa cada una de ellas.

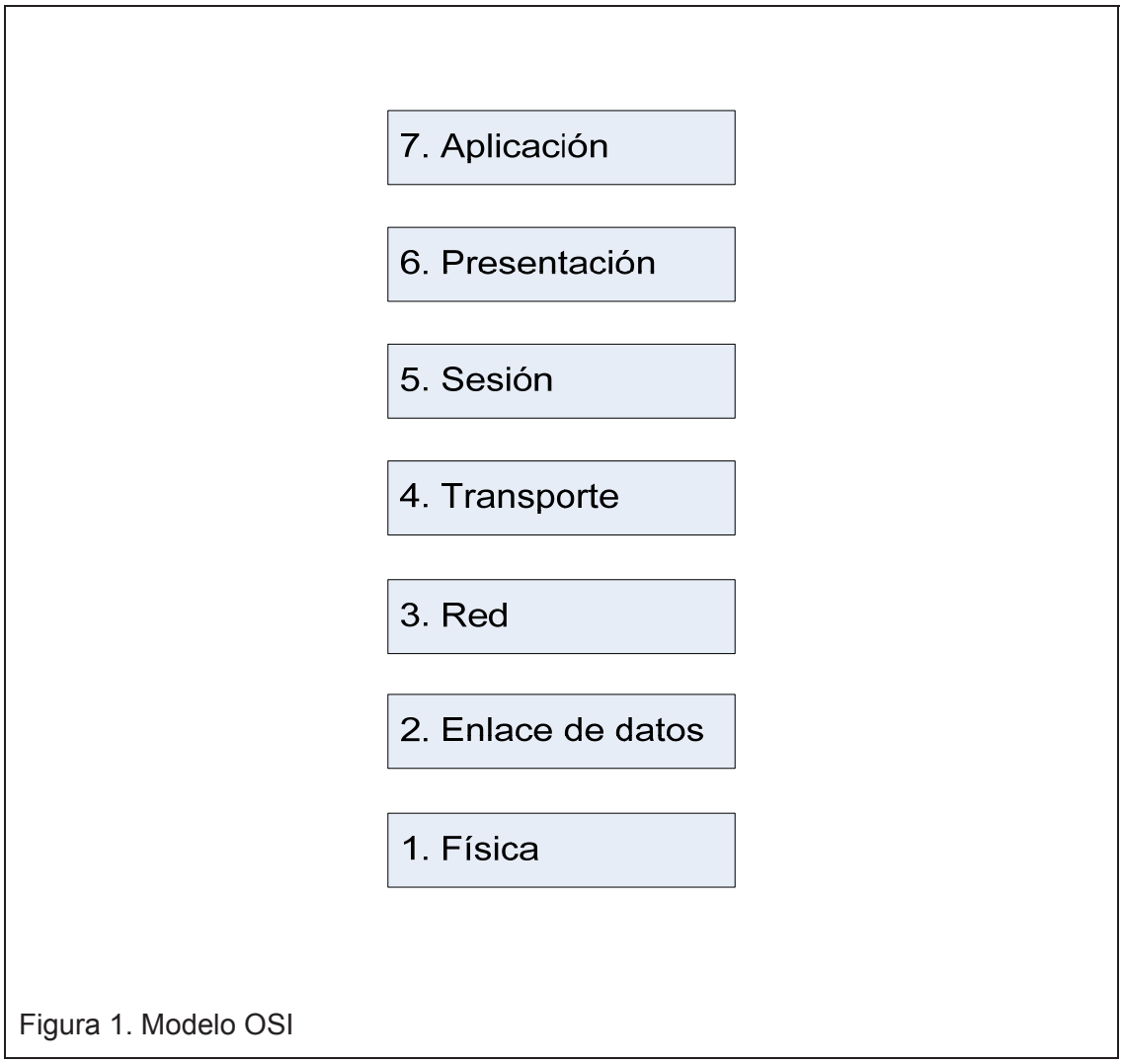


Figura 1. Modelo OSI

Para poder comprender el funcionamiento de las aplicaciones mencionadas la organización de estándares internacionales desarrolla un modelo en capas que ha servido a los profesionales de telecomunicaciones y programadores para diseñar programas y resolver problemas. El sistema propuesto lo llamaron Interconexión de Sistema Abierto o más conocido como modelo OSI.

1.2 Capa de aplicación

Las aplicaciones que los usuarios utilizan como navegadores web, herramientas de correo, sistemas de información son las que permiten acceder a los servicios de red y conectarse con la capa de presentación, los protocolos que se ejecutan son HTTPS, POP, SMTP, SMTP, DHCP, entre otros, adicionalmente se ejecutan servicios como DNS, SSH, TELNET.

1.3 Capa de presentación

Esta capa se caracteriza por convertir y codificar los datos que entrega la capa de superior garantizando que los datos de la unidad de origen sean descifrados por la aplicación indicada en la unidad de destino. Por otra parte se encarga de comprimir los datos que entrega el dispositivo de origen y que puedan ser descomprimidos por el terminal de destino.

Los protocolos que operan en esta capa son SSL, TSL. Los servicios que se ejecutan son JPEG, GIF, MPEG, en la labor de compresión de datos estarían los programas compresores RAR, ZIP.

1.4 Capa de sesión

En esta capa se crea y establece comunicación permanente entre aplicaciones de origen y destino intercambiando información para iniciar diálogos y conservarlos activos. Otra acción que se ejecuta en esta capa es la de reiniciar

sesiones que se desactivaron o se interrumpen durante un espacio de tiempo extenso.

Los protocolos que se ejecutan en esta son NFS, SQL, RPC, ASP, DNA SCP.

1.5 Capa de transporte

En esta capa se encapsulan los datos que se generan en la capa aplicación con el fin de ser usados en la capa de red, permite múltiples aplicaciones para comunicarse por medio de la red en un solo dispositivo al mismo tiempo.

Asegura que la data sea recibida de forma confiable y ordenada por la aplicación, además utiliza elementos de manejo de error.

La figura 2 muestra la ubicación de la capa de transporte y su funcionalidad dentro del modelo OSI.

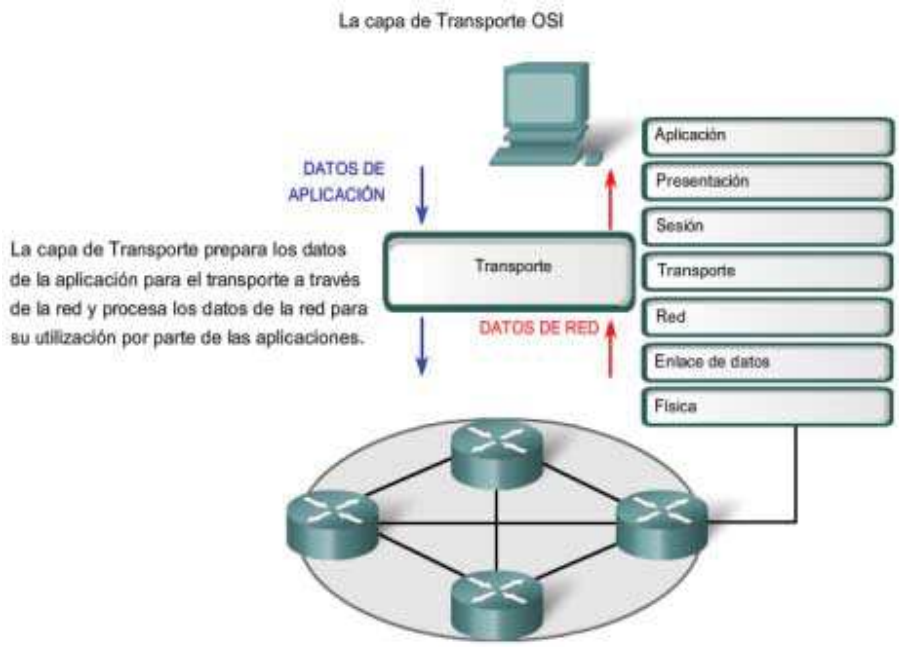


Figura 2. Capa de transporte
Tomado de Cisco Networking Academy, 2013

En la figura 3, se detalla el propósito de la capa de transporte una vez conocido que en esta capa se realiza la segmentación de los datos realizando el control necesario para reagrupar las partes dentro de los diferentes circuitos de comunicación.

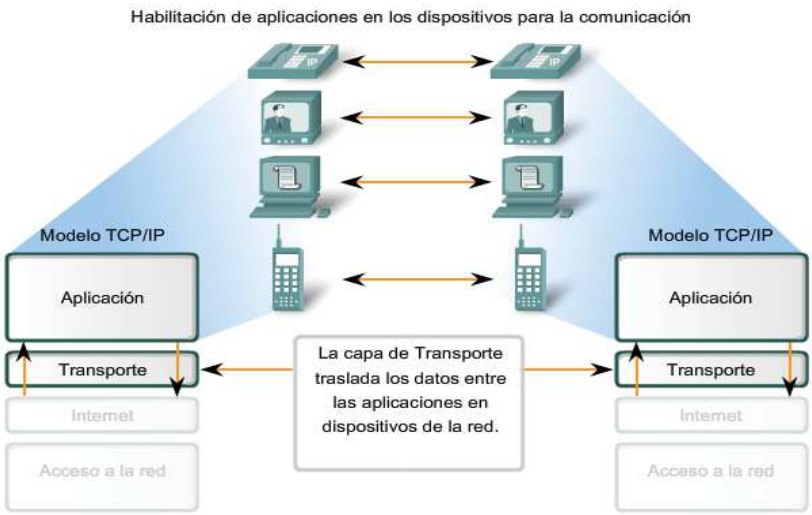


Figura 3. Propósito de la capa de transporte

Tomado de Cisco Networking Academy, 2013

Como se puede observar cualquier equipo puede mantener múltiples aplicaciones que necesitan comunicarse a través de la red con sus equipos donde se origina el servicio pedido, es así que se considera como responsabilidad de esta capa mantener los circuitos de comunicación entre las aplicaciones solicitadas.

La segmentación de datos pasa a ser una de las responsabilidades de esta capa debido a que cuando se generan los circuitos de datos entre aplicación local y remota estos deben ser preparados y enviados por un medio de transmisión en partes manejables.

El reemsamble de segmentos se lo realiza en el equipo que recibe la data, cada sección de datos se lo direcciona a la aplicación adecuada, los protocolos

que se ejecutan en esta capa detallan como utilizar la información de los encabezados para reemsamblar las secciones de datos en circuitos y enviar a la capa de aplicación.

Cuando se quiere transferir un conjunto datos a las aplicaciones adecuadas, una de las forma como se envía es a través de la identificación de la aplicación de destino, asignando en la capa de transporte un identificador por cada aplicación, usualmente se utiliza la identificación por número de puerto a cada una de las aplicaciones.

Concluyendo el tema se puede decir que la capa de transporte pasa a ser una de las más importantes en este modelo en capas, ya que permite la conexión entre la capa de aplicación y el resto de capas del modelo OSI que se encargan de la envío de datos en la red.

En la figura 4, se observa como la capa de transporte se encarga de separar las múltiples conversaciones que se ejecutan en un host, realizando el seguimiento de ellas y procurando que las diferentes aplicaciones solicitadas sean entregadas completas y al destinatario indicado.

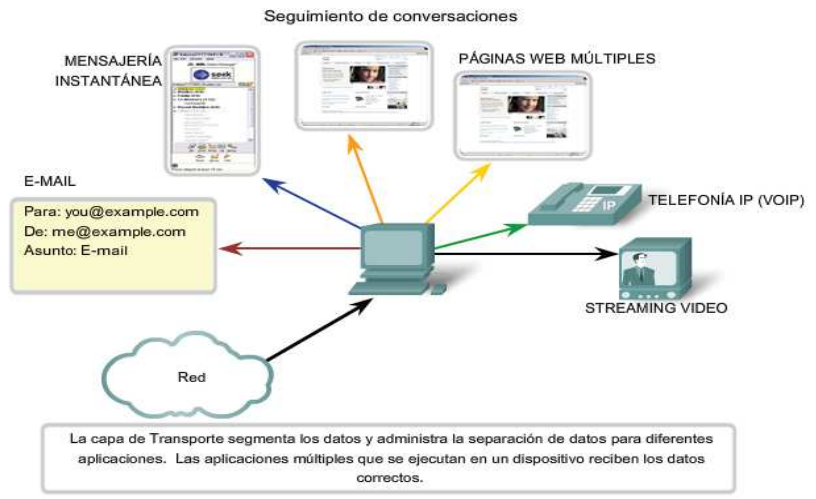


Figura 4. Seguimiento de conversaciones
Tomado de Cisco Networking Academy, 2013

Para hablar acerca de la segmentación que se produce sobre un medio de comunicación pasa a ser primordial en la capa de transporte y que mediante la segmentación permite que se ejecuten múltiples aplicaciones de manera concurrente en una computadora. Para identificar cada uno de los circuitos de datos enviados la capa de transporte lo que hace es agregar un encabezado que contiene datos binarios, en la figura 5 se muestra algunos de los segmentos con datos binarios.

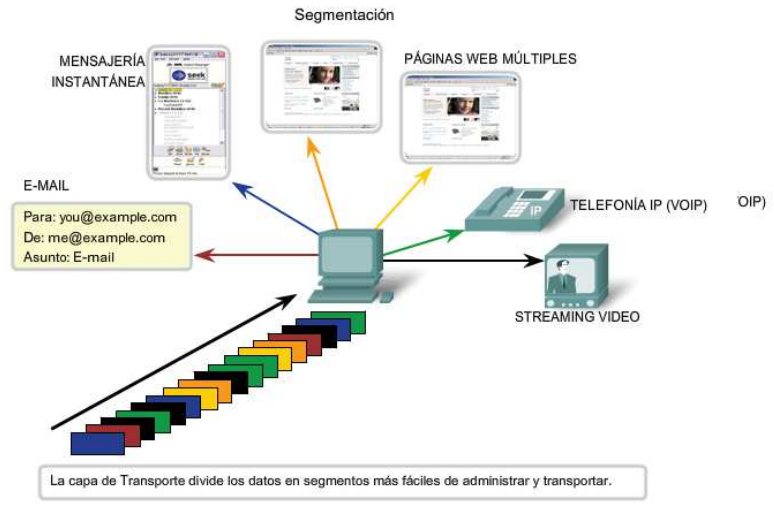


Figura 5. Identificación de los segmentos con datos binarios
Tomado de Cisco Networking Academy, 2013

1.5.1 Control de conversaciones

Una vez que se ha revisado segmentación, seguimiento, reensamblaje y multiplexación de la data, ahora nos toca hablar de donde se proveen los protocolos.

Antes de transmitir información previamente se crea una sesión orientada a la conexión entre las aplicaciones, obteniendo una mejor gestión de los datos entre las aplicaciones.

La entrega confiable de paquetes garantiza la capa de transporte asegurándose que todos los datos lleguen al destino y de ser necesario solicitar al origen la retransmisión de la data.

Otro de los procedimientos acertados de esta capa es la entrega de la data en el mismo orden, al momento que identifica y secuencia los segmentos, la capa de transporte puede asegurar que estos se vuelvan a ordenar tal como fueron enviados por el origen.

El control de flujo es también manejado por la capa de transporte regulando la cantidad de data que el origen transmite como grupo ayudándonos a prevenir la perdida de segmentos en la red evitando la necesidad de retransmisión de datos.

En la figura 6 se muestra algunos de los servicios que se ejecutan en la capa de transporte.

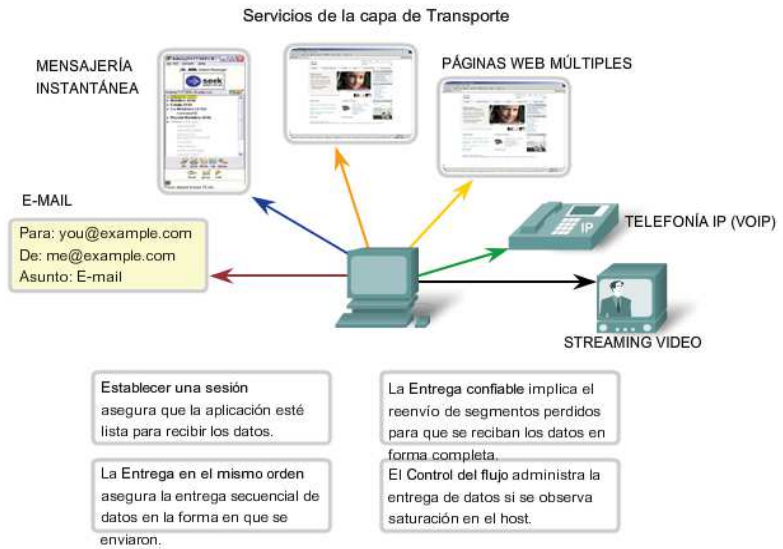


Figura 6. Funciones realizadas en la capa de transporte
Tomado de Cisco Networking Academy, 2013

Ahora se indicará los protocolos que se ejecutan en la capa de transporte siendo TCP y UDP los más destacados.

El protocolo de datagramas de usuario o mejor conocido como UDP es simple y es no orientado a la conexión, una de sus ventajas es que entrega los paquetes si necesitar de muchos recursos. Las porciones de comunicación en este protocolo se llaman datagramas y son enviados como “mejor intento”.

Aplicaciones como los servidores de nombres de dominio, archivos de video y voz utilizan al protocolo UDP como su protocolo de transmisión de datos.

El protocolo de control de transmisión o mejor conocido como TCP es orientado a la conexión que se ejecuta en la capa de transporte, cumple funciones adicionales como entrega confiable y control de flujo de segmentos.

Las aplicaciones que se sirven de TCP son las ya conocidas como los navegadores web, email, ftp, telnet, etc.

En la figura 7, se encuentra un segmento TCP compuesto por 20 bytes de cabecera en el encabezado, encargándose de encapsular los datos de la capa de aplicación, en tanto que en cada segmento UDP posee únicamente 8 bytes de cabecera.

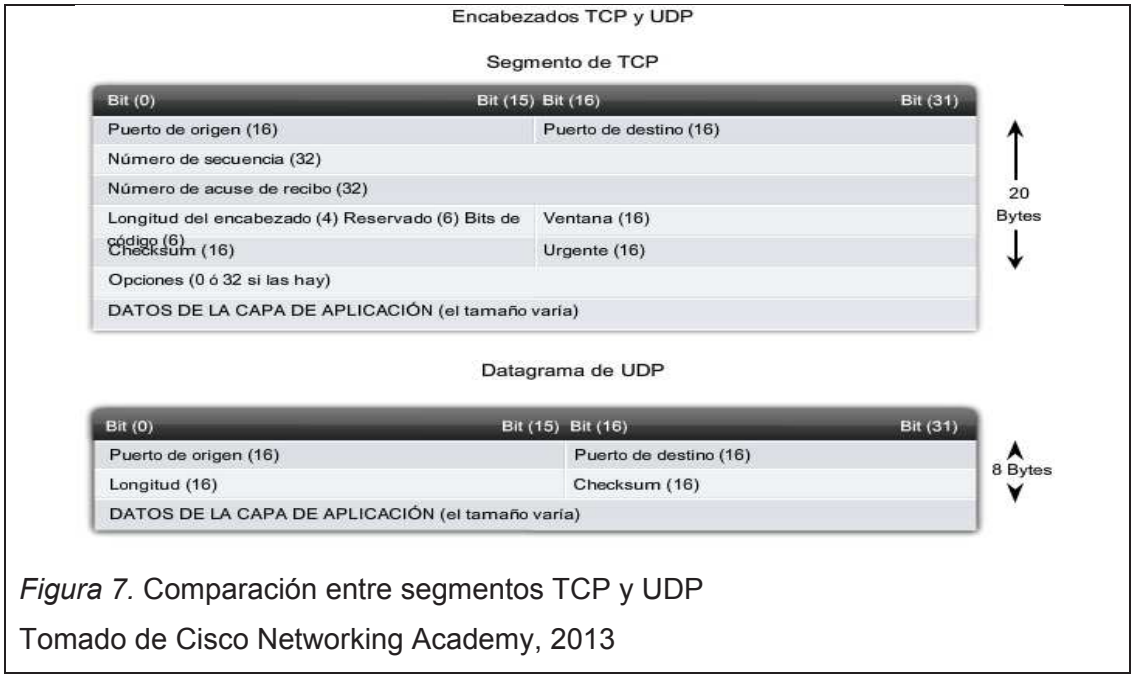


Figura 7. Comparación entre segmentos TCP y UDP
Tomado de Cisco Networking Academy, 2013

1.5.2 Direccionamiento del puerto

En la capa de transporte de consideró establecer de mejor forma las sesiones entre las aplicaciones asignando tanto en TCP como en UDP campos de encabezado para identificar de manera exclusiva las aplicaciones, a estos identificadores los llamaron puertos.

En la figura 8, encontrarán la asignación de puertos a aplicaciones, cabe recalcar que quien administra estos puertos es la IANA (Internet Assigned Numbers Authority) que es la encargada de coordinar la raíz global de DNS, el direccionamiento IP, protocolos de internet.

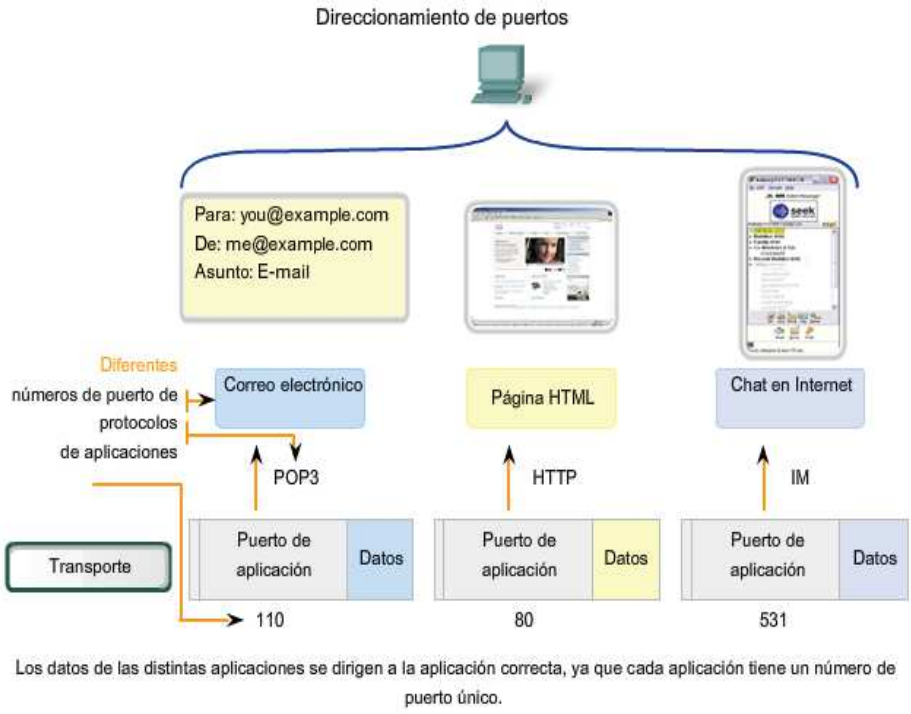


Figura 8. Identificación de aplicaciones con número de puerto
Tomado de Cisco Networking Academy, 2013.

La forma como responde una aplicación asignada un número de puerto se la describe a continuación, usualmente una aplicación cliente envía una solicitud de servidor, el puerto destino contenido en el encabezado es el número de

puerto que se asigna al demonio de servicio que se ejecuta en el host remoto. La aplicación del cliente debe conocer el número de puerto asociado con el proceso del servidor en el host remoto.

1.6 Capa de red

Uno de los temas más importantes en esta capa es el direccionamiento y los procesos que permiten que los datos de la capa de transporte sean empaquetados y transportados hacia las capas inferiores, a continuación se revisarán de forma general cual es la función de la capa de red, para posteriormente desarrollar de una forma más amplia el protocolo IPv4.

Los procedimientos que se utilizan para transportar los datos de host a hosts son direccionamiento, encapsulamiento, enrutamiento y desencapsulamiento.

Para transportar datos de un terminal a otro una condición indispensable es que cada uno de estos debe tener una dirección única, al momento de asignar esta dirección al terminal se lo denomina host. La encapsulación de datos pasa a ser el segundo paso para el transporte de datos ya que los host no deben ser identificados únicamente con una dirección, la capa de red recibe los segmentos de la capa de transporte y se agrega una etiqueta de capa de red para crear los paquetes de la capa de red. La etiqueta de la capa de red debe contener la dirección de host a la que se está enviando o más conocida como dirección destino cabe recalcar que en la etiqueta debe contener también la dirección del host origen.

El tercer paso es el enrutamiento, la capa de red debe conocer por donde enviar los paquetes al host destino, los dispositivos que nos ayudan a seleccionar las rutas y dirigir paquetes hacia su destino son los enrutadores, estos son capaces de conocer dispositivos que se encuentre en interconectando redes.

Por último el desencapsulamiento se lo realiza cuando el host destino examina la dirección de destino para verificar que el paquete fue enviado a ese terminal, en caso de ser correcto el paquete es desencapsulado por la capa de red y los segmentos de la capa de transporte contenida en el paquete.

Los protocolos que se ejecutan en la capa de red que llevan datos del usuario se los menciona a continuación:

- Protocolo IPv4
- Protocolo IPv6
- Appletalk
- Servicio de red sin conexión CLNS/DECNet
- IPX

1.7 Capa de enlace de datos

En la figura 9, se muestra algunos términos específicos para esta capa como trama, nodo, medio físico, red.

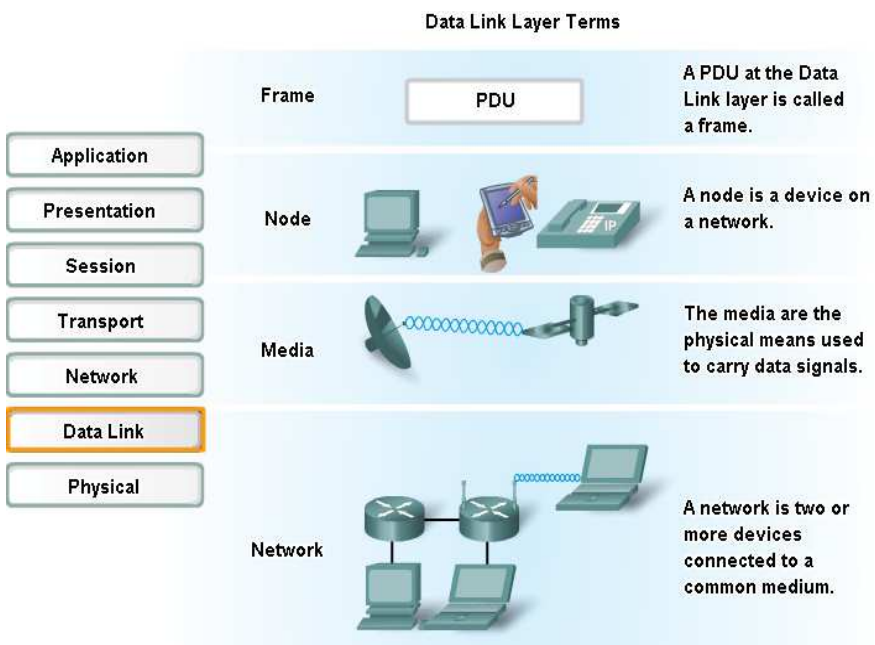


Figura 9. Identificación de aplicaciones con número de puerto
Tomado de Cisco Networking Academy, 2013

Esta capa cumple una tarea importante ya que se encarga de preparar y controlar los paquetes a ser transmitidos convirtiéndolos en tramas desde la capa de red hacia la capa física.

1.7.1 Subcapas de la capa de enlace

Otro de los temas importantes a tomar en cuenta son las subcapas de enlace de datos para redes LAN entre ellas se enlistará a algunas de ellas.

LLC conocido también como control de enlace lógico, en esta se coloca información en la trama que identifica que protocolo de capa de red está siendo utilizado en la trama.

La otra subcapa es la dirección MAC la misma que “proporciona a la capa de enlace de datos el direccionamiento y la delimitación de datos de acuerdo con los requisitos de señalización física del medio y al tipo de protocolo de protocolo de capa de enlace de datos en uso”. Cisco Networking Academy. (2013).

En la figura 10 se muestra las subcapas que conforma a enlace de datos, entre ellas al control de enlace lógico y acceso al medio.

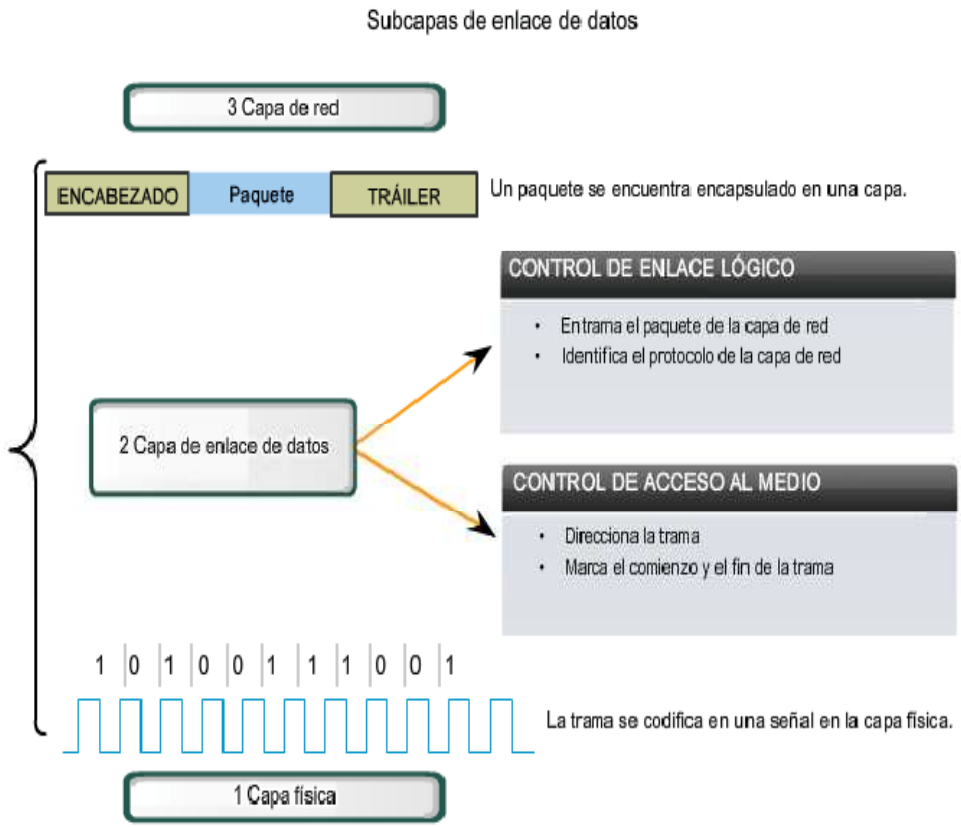


Figura 10. Subcapas de enlace de datos
Tomado de Cisco Networking Academy, 2013

1.7.2 Estándares de la capa de enlace de datos

En las capas superiores se ha venido revisando los protocolos y servicios que se ejecutan en cada una de ellas, para el caso de la capa enlace de datos existen los estándares propuestos por empresas de estandarización como ISO, IEEE, ANSI, ITU, ellos normaron que en la capa dos los procesos se producen tanto en el software como en el hardware, es así que los protocolos de la capa de enlace de datos se ejecutan dentro de la electrónica de los adaptadores de red mediante el cual los host se conecta a la red física.

En la tabla 1, se muestra algunos de los estándares normalizados para la capa dos.

Tabla 1. Subcapas de enlace de datos

EMPRESA	ESTANDAR
ISO	HDLC (High Level Data Link Control)
IEEE	802.2 (LLC) 802.3 (Ethernet) 802.5 (Tokeng Ring) 802.11 (Wireless LAN)
ITU	Q.922 (Frame Relay Standard) Q.921 (ISDN Data Link Standard) HDLC (High Level Data Link Control)
ANSI	3T9.5 ADCCP (Advanced Data Communications Control Protocol)

Tomado de Cisco Networking Academy, 2013

1.8 Capa física

La capa física del modelo OSI un sistema de comunicaciones es la que se encarga de codificar en señales eléctricas los dígitos binarios que representan las tramas de la capa dos, adicionalmente recibe y transmite señales eléctricas de los medios de transmisión que conectan los dispositivos de la red.

Como tarea importante de la capa física es transformar la representación de bits de cada trama en señales ópticas, eléctricas o de microondas, una vez que se realiza este proceso las señales están listas para ser enviadas por los medios de transmisión, cosa parecida sucede cuando una señal eléctrica, óptica o de microondas debe pasar a ser bits para su posterior composición en tramas y enviar a la capa de enlace de datos.

En la figura 11, se muestra las transformaciones mencionadas.

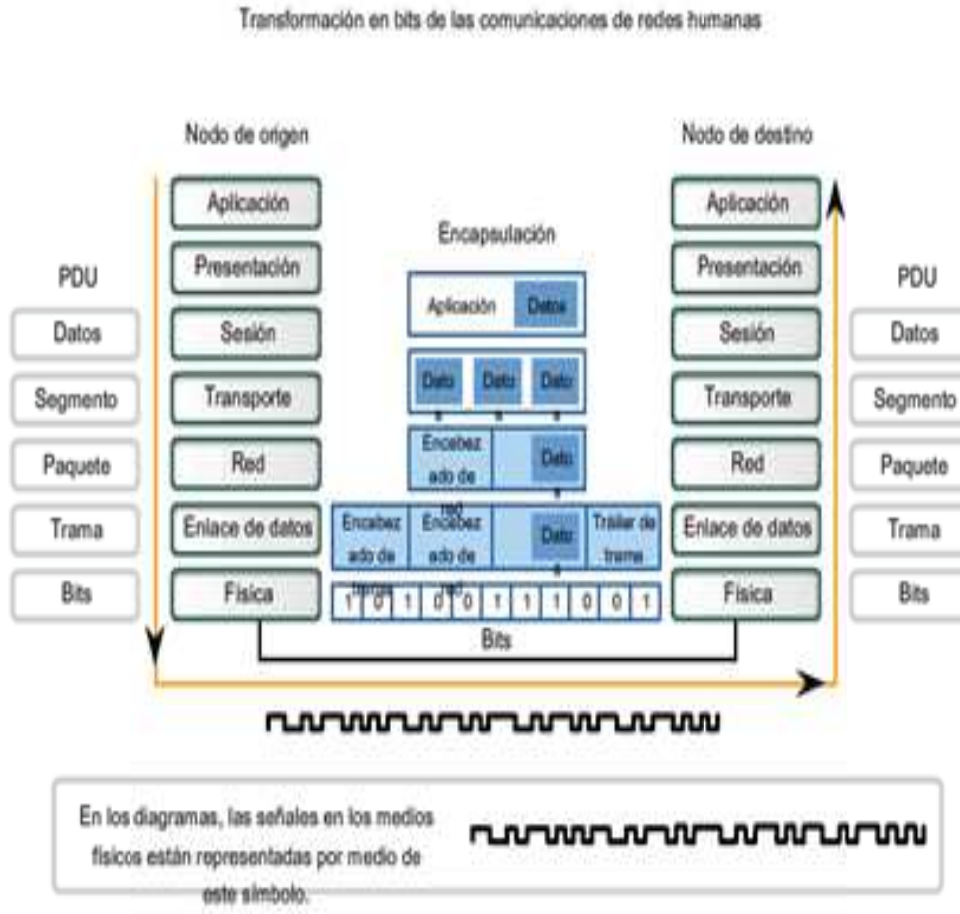


Figura 11. Transformación de bits a señales eléctricas y viceversa
Tomado de Cisco Networking Academy, 2013

Ahora se tomará en cuenta cómo se transportan las tramas al momento de ser transformadas a señales eléctricas, para estos anunciaremos a los medios de transmisión básicos que existe como el cable de cobre, fibra óptica e inalámbrico o microondas, cabe indicar que para cada uno de estos medios el tipo de señal varía es decir que para sistemas de fibra óptica la señal será luz, para cobre pulsos eléctricos y para medios inalámbricos ondas electromagnéticas.

En la figura 12, se identifica cada una de las señales mencionadas realizando una representación de estas.

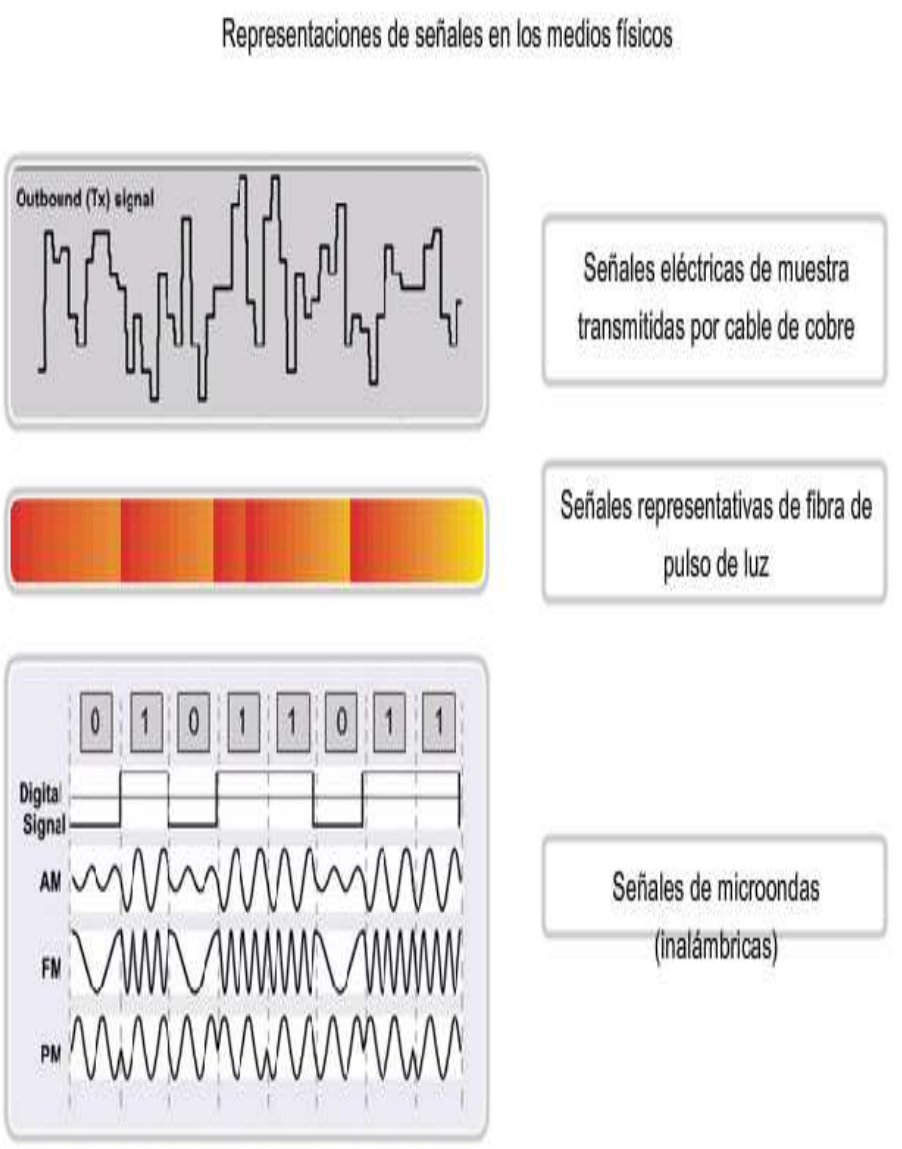


Figura 12. Representación de señales eléctricas en los medio de transmisión
Tomado de Cisco Networking Academy, 2013

1.8.1 Estándares de la capa física

Debido a que esta capa interactúa directamente con medios de transmisión físicos dentro de los cuales están los conectores, cables o medios, circuitos eléctricos se hace necesario que exista una norma para la construcción de estos, por lo que instituciones como ISO, IEEE, ANSI, ITU, EIA/TIA, FCC deciden estandarizar los medios mencionados en los que se especifica los requisitos de cableado, conectores y señales eléctricas.

En la figura 13, se muestra los elementos a ser estandarizados.

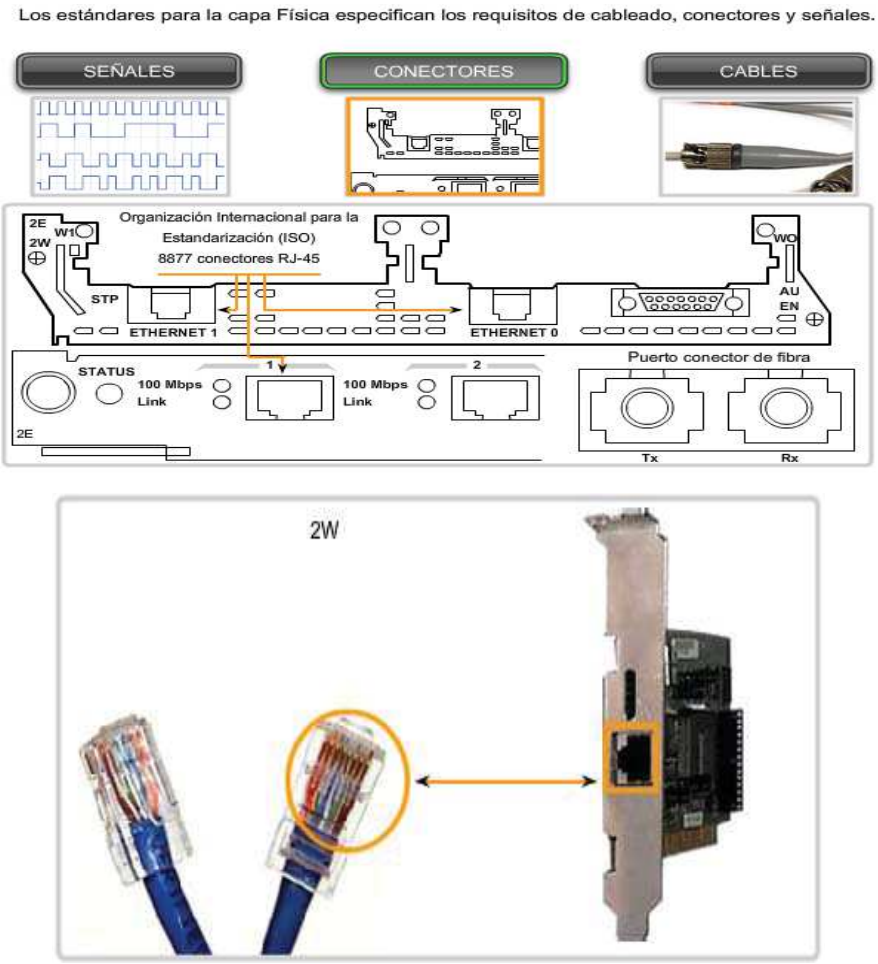


Figura 13. Elementos a ser estandarizados

Tomado de Cisco Networking Academy, 2013

1.8.2 Principios fundamentales de la capa física

Para estos es necesario indicar tres funciones esenciales de la capa física como los componentes físicos que son los dispositivos electrónicos de hardware, conectores, medios que transmiten y transportan las señales para representar los bits.

La segunda función es la codificación siendo esta un método utilizado para convertir un conjunto de bits de datos en código predefinido, adicionalmente en la capa física puede crear códigos para identificar el comienzo y el final de una trama.

Como tercera función y última es la señalización, considerada como representaciones de 1 o 0 que debe generar las señales que transportan datos en la capa física.

En la figura 14, se muestra las funciones mencionadas.

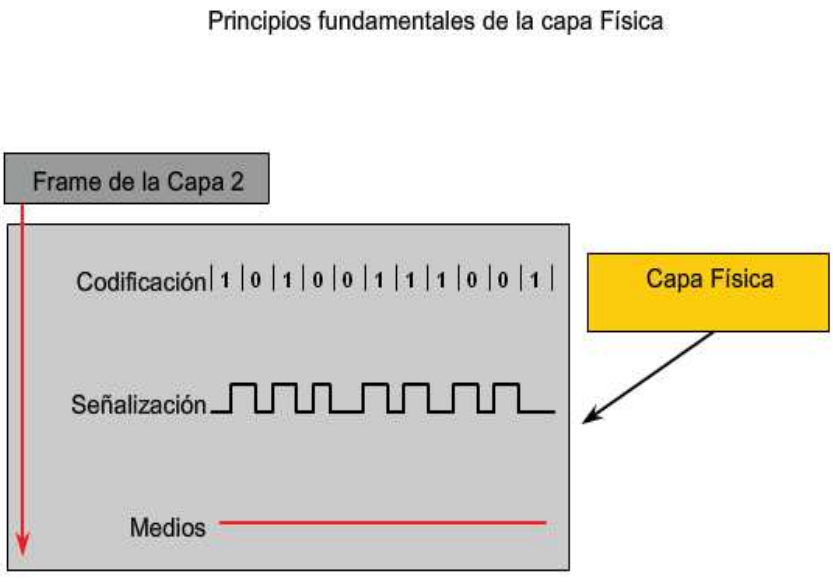


Figura 14. Representación de los datos en la capa física
Tomado de Cisco Networking Academy, 2013

Es así como hemos podido revisar de una manera general las capas de modelo OSI consideradas como fundamentales para el estudio de un sistema de telecomunicaciones, ahora se analizará ampliamente el protocolo IPv4, importante en la elaboración del trabajo de titulación propuesto.

1.9 IPv4

IPv4 es un protocolo de la capa de red del modelo OSI que fue diseñado como de bajo costo, su función es la de enviar un paquete desde un host origen a un host destino a través de un red interconectada.

Haciendo referencia a la figura 15, se describe a IPv4 como un protocolo sin conexión lo que significa que los paquetes IP se envían sin notificar al host de destino que está llegando, al no tener esta notificación podemos obtener como resultado que los paquetes no lleguen a su destino de forma secuencial u ordenada, provocando que las capas superiores tengan que solicitar la retransmisión de la información.

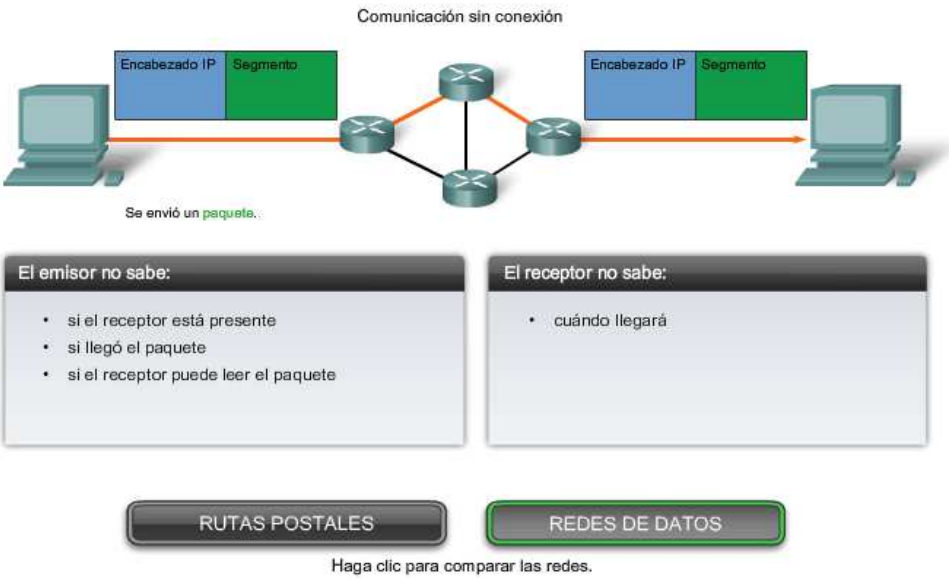


Figura 15. Comunicación sin conexión

Tomado de Cisco Networking Academy, 2013

Otra de las características de IPv4 es que es un protocolo no confiable o también llamado de servicio de mejor intento, lo que significa este no tiene la capacidad de administrar ni recuperar paquetes corruptos o no entregados. Quienes se encargan de realizar el control de errores son los protocolos de las capas superiores.

En la figura 16, se muestra una ilustración acerca de esta característica.

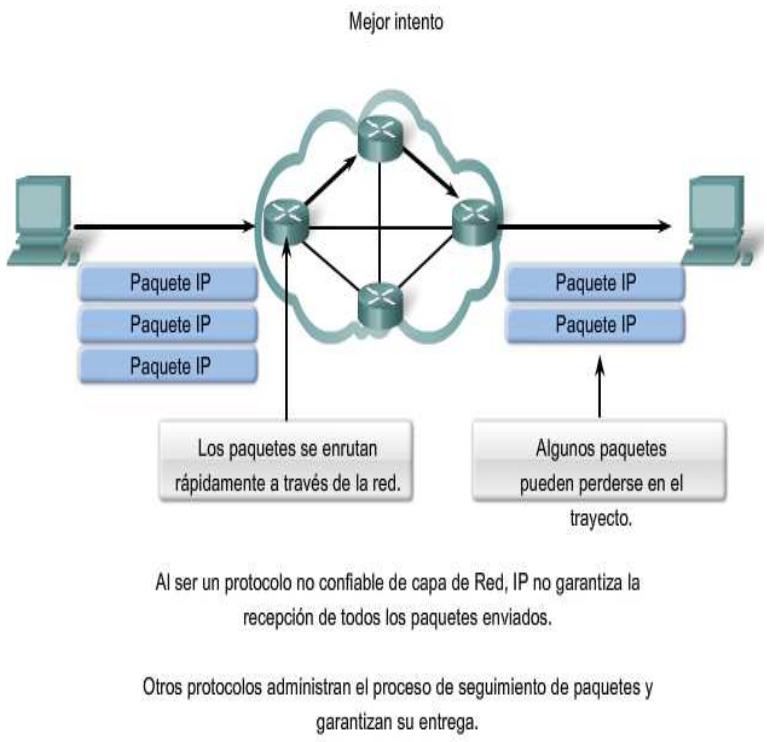


Figura 16. Comunicación de mejor intento.
Tomado de Cisco Networking Academy, 2013

La tercera característica de IPv4 se describe como un protocolo independiente de los medíos de transmisión, para la capa física no le interesa las características de los medios mediante los cuales se transporta los paquetes, existe un parámetro que la capa física que si lo considera importante que es la MTU o denominado también tamaño máximo de la PDU que cada medio puede transportar, muchas veces se necesita de un dispositivo intermedio para

acoplar el medio en caso que se debiera separar un paquete cuando se lo envía desde un medio de transmisión a otro medio de transmisión con un MTU más pequeña.

Como se muestra en la figura 17, varios medios de comunicación sea con cable de cobre, fibra óptica o inalámbrica.

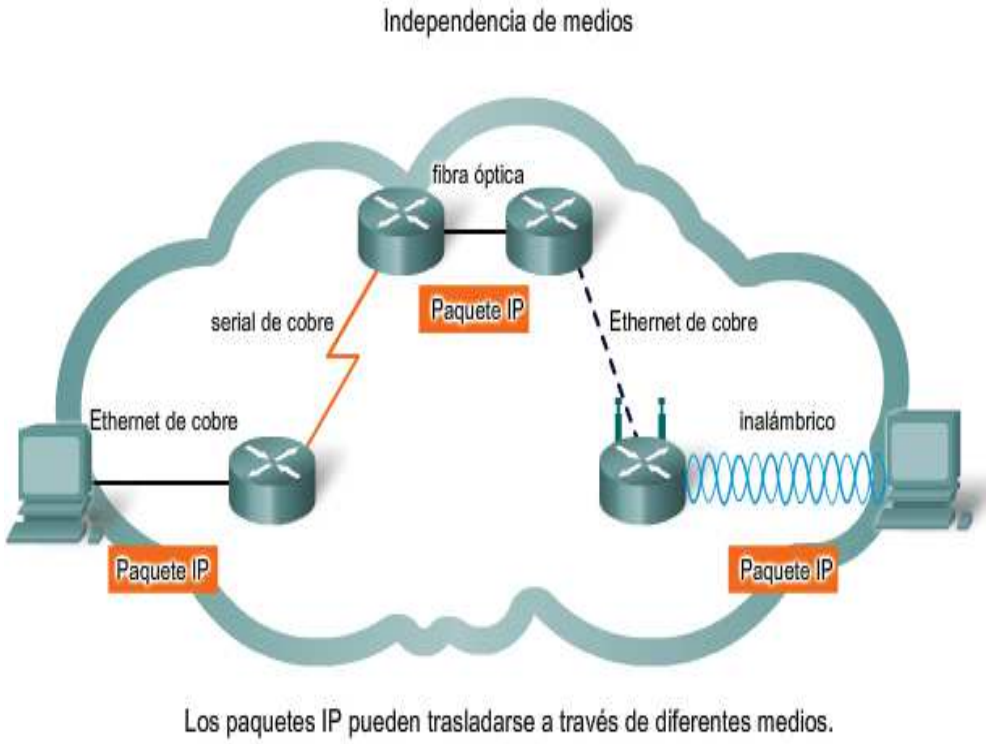


Figura 17. Independencia de los medio de transmisión
Tomado de Cisco Networking Academy, 2013

1.9.1 Encapsulación de la PDU de la capa de transporte

El proceso de encapsulación de los segmentos de la capa de transporte en el protocolo IPv4 se lo realiza con el fin de que la red pueda entregar los datos transportados a su host de destino.

Al realizar el proceso de encapsulación permite que los servicios en las diferentes capas funcionen sin afectar a otras, y que los protocolos de la capa de red puedan empaquetar fácilmente los segmentos de la capa de transporte, adicionalmente se considera que la PDU encapsulada de la capa cuatro del modelo OSI durante el procesos de la capa de red permanezcan intactos.

En la figura 18 se muestra el proceso señalado.

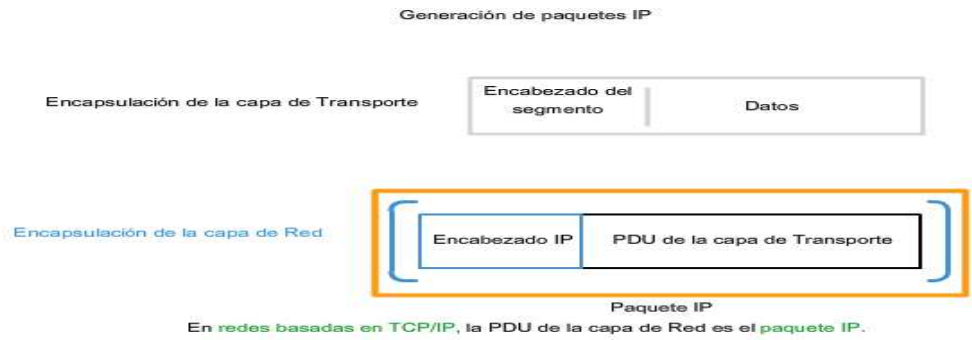


Figura 18. Encapsulación de paquetes en IPv4.
Tomado de Cisco Networking Academy, 2013

1.9.2 Encabezados del paquete IPv4

Para analizar este tema se tomará en cuenta la figura 19.

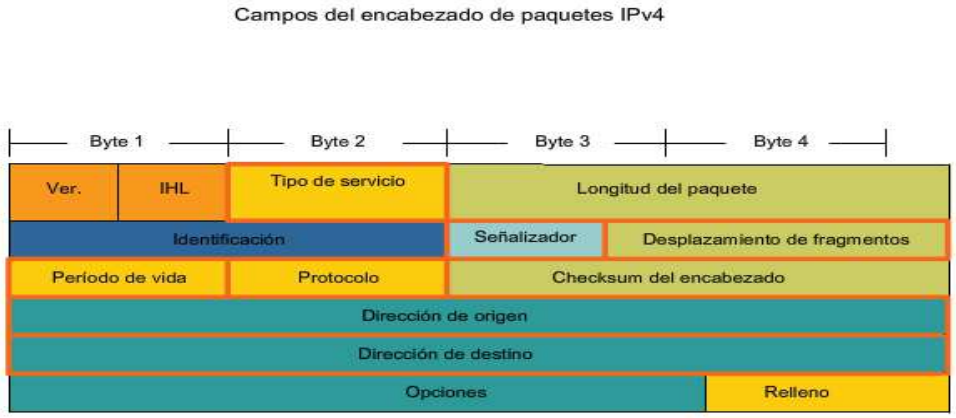


Figura 19. Campos del encabezado IPv4
Tomado de Cisco Networking Academy, 2013

Los campos a tomar en cuenta son los siguientes:

La dirección IP origen está compuesta por un valor binario de 32 bits que representa la dirección de host de la capa de red de origen de paquete.

La dirección IP destino está formada por un valor binario de 32 bits representando la dirección de host de la capa de red de destino del paquete.

El campo TTL o más conocido como el tiempo de vida está formado por un valor binario de 8 bits que indica el tiempo que queda de vida del paquete, cada vez que pasa por un enrutador este disminuye en uno hasta que se haga cero en este instante el paquete se elimina cortándose el flujo de datos de la red.

El campo protocolo está compuesto por un valor binario de ocho bits e indica el tipo de relleno de carga que el paquete traslada.

El campo tipo de servicio tiene un valor binario de 8 bits usado para determinar la marcación de cada paquete.

El campo desplazamiento de fragmentos y el señalizador de MF en el encabezado IP, es utilizado porIPv4 para realizar la reconstrucción del paquete cuando llega a su host de destino. En si el campo de desplazamiento del fragmento identifica el orden en el cual ubicar el fragmento de paquete en el reconstrucción.

El campo señalizador de más fragmentos (MF) es un único bit en el campo del señalizador usado con el desplazamiento de fragmentos para la fragmentación y reconstrucción de paquetes.

El señalizador de no fragmentar (DF) es un solo bit que se lo encuentra dentro del campo señalizador, su función es la de indicar que no se permite la fragmentación de paquetes, para permitir el paso de paquetes fragmentados

hacia la capa de enlace de datos un enrutador debe poner en 1 el bit DF para posteriormente descartar el paquete.

Adicionalmente se enlistan otros campos que forman parte del encabezado de IPv4:

Versión: este contiene el número IP de la versión (4).

Longitud del encabezado (IHL): especifica el tamaño del encabezado del paquete.

Longitud del paquete: este campo muestra el tamaño completo del paquete, incluyendo el encabezado y los datos, en bytes.

Identificación: este campo es principalmente utilizado para identificar únicamente fragmentos de un paquete IP original.

Checksum del encabezado: este campo se utiliza para controlar errores del encabezado del paquete.

Opciones: La RFC 791 define al campo opciones como de longitud variable y es pocas veces utilizado, son útiles en algunas situaciones, incluyen recursos para marcas de tiempo, seguridad y encaminamiento especial.

1.9.3 Direccionamiento IPv4

Cada uno de los hosts que componen una red deben estar identificados con una dirección única, de tal forma que la comunicación entre equipos sea entre IP origen e IP destino, para que de esta forma la capa de red pueda identificar los paquete enviados y recibidos.

Una dirección IPv4 está compuesta de una porción de red y una porción de hosts, formada por cuatro grupos de 8 bits denominados octetos separado por un punto decimal, pueden ser escritos ya sea de forma decimal o binaria.

En la tabla 2 se indica un ejemplo de cómo se representa una dirección IPv4.

Tabla 2.Representación de direcciones IPv4

Representación	**Notación**
Decimal	172.16.112.11
Binaria	10101100.00010000.11100000.00001011

Tomado de Cisco Networking Academy, 2013

1.9.4 Tipos de direcciones IPv4

Como objeto de estudio diremos que una dirección de red hace referencia a toda la red mediante la dirección más baja, una dirección de broadcast usualmente es la dirección más alta de la red, es usada para enviar datos a todos los hosts de la red al mismo tiempo. Las direcciones de hosts son las que se asignan a los equipos activos que conforman una red.

En la tabla 3 se muestra los tipos de direcciones citadas:

Tabla 3. Tipos de direcciones IPv4

Dirección	**Notación**
Red	172.18.112.0
Broadcast	172.18.112.255
Host	172.18.112.154

Tomado de Cisco Networking Academy, 2013

1.9.5 Mascara de red

La máscara nos permite identificar un rango de direcciones IPv4 e indicar la porción de red y la porción de host, conocido también como prefijo de red

compuesta de 32 bits, la representación que se le ha dado es en forma de bits binarios es decir 24 bits, 16 bits, 8 bits, etc.

1.9.6 Tipos de comunicación

La forma en la que los hosts se comunican dentro de una red IPv4 es de tres maneras:

Al proceso de envío de un paquete de un host a otro host de forma individual se conoce como tráfico unicast.

Cuando un paquete es transmitido desde un host a todos los hosts de una red se conoce como transmisión broadcast.

Enviar un paquete desde un hosts a un grupo de hosts seleccionado se lo conoce como transmisión multicast.

1.9.7 Direccionamiento IPv4

Existen dos tipos de direccionamiento IPv4,direccionamiento público y privado, las direcciones públicas son designadas para equipos que se exponen a Internet y su acceso es público, las direcciones IPv4 privadas usualmente se encuentran asignadas en equipos que no están expuestos directamente a Internet.

Existen rangos de IPv4 considerados como privados y que al momento de configurar una red de tipo privada deben ser usadas de manera obligatoria.
En la tabla 4, se muestra los bloques de direcciones IPv4 consideradas como privadas.

Tabla 4. Bloques de direcciones IPv4 privadas

10.0.0.0	a	10.255.255.255
172.16.0.0	a	172.31.255.255
192.168.0.0	a	192.168.255.255

Tomado de Cisco Networking Academy, 2013

Existen otros tipos de direcciones IPv4 consideradas como especiales:

- Ruta predeterminada (Ej. 0.0.0.0)
- Dirección de loopback (Ej. 127.0.0.1)
- Direcciones de enlace local (Ej. 169.254.0.0 a 169.254.255.255)
- Direcciones de TEST-NET (Ej. 192.0.2.0 a 192.0.2.255)

1.9.8 Direccionamiento con clase

Se define como direccionamiento con clase a bloques de direcciones limitadas por tamaños específicos, en la figura 20 se muestra los diferentes bloques de direcciones sus direcciones de inicio y fin.

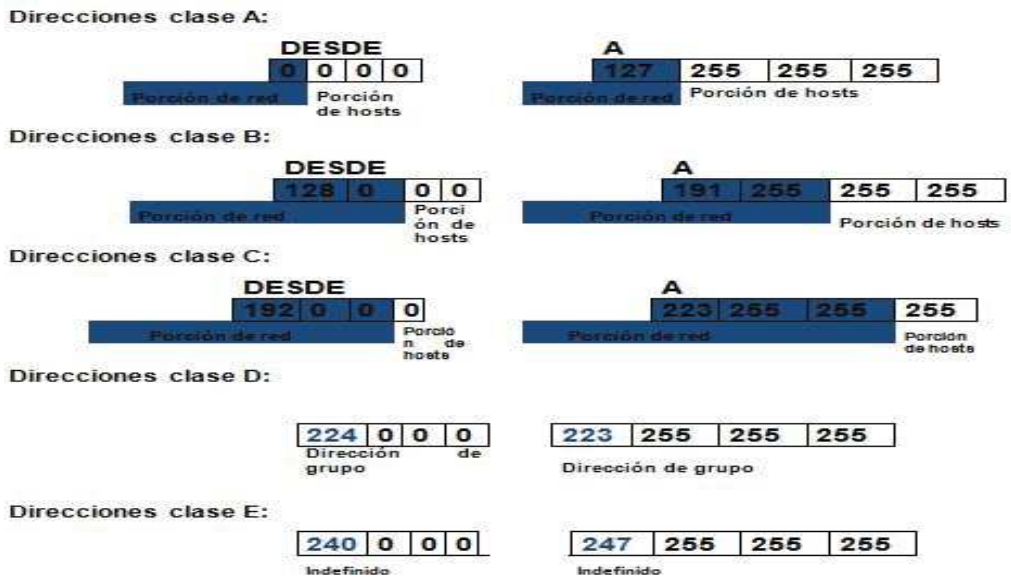


Figura 20. Campos del encabezado IPv4

Tomado de Cisco Networking Academy, 2013

1.9.9 Direccionamiento sin clase

Con este direccionamiento lo que se trata de hacer es ajustar los bloques de direcciones IPv4 a los números de hosts necesarios para una red.

En la tabla 5, se muestra las posibles subredes que se pueden obtener de las redes con clase.

Tabla 5.Subredes de las redes con clase

IP Address Classes

Address Class	1st octet range (decimal)	1st octet bits (green bits do not change)	Network(N) and Host(H) parts of address	Default subnet mask (decimal and binary)	Number of possible networks and hosts per network
A	1-127**	00000000-01111111	N.H.H.H	255.0.0.0	128 nets (2^7) 16,777,214 hosts per net (2^24-2)
B	128-191	10000000-10111111	N.N.H.H	255.255.0.0	16,384 nets (2^14) 65,534 hosts per net (2^16-2)
C	192-223	11000000-11011111	N.N.N.H	255.255.255.0	2,097,150 nets (2^21) 254 hosts per net (2^8-2)
D	224-239	11100000-11101111	NA (multicast)		
E	240-255	11110000-11111111	NA (experimental)		

** All zeros (0) and all ones (1) are invalid hosts addresses.

Tomado de Cisco Networking Academy, 2013

Con el direccionamiento sin clase se trata de evitar desperdiciar direcciones IPv4, los diseños de red deben ser realizados para en lo posible se optimice el uso de direcciones, es decir que si una empresa necesita un grupo de direcciones para 300 hosts, estas deberán ser calculadas para cubrir estrictamente esta necesidad, siendo esta la razón para que exista la división de los direccionamientos con clases en direccionamientos más pequeños conocido ahora como direccionamiento sin clase.

1.9.10 Distribución de direcciones IPv4 en el mundo

Las empresas que deseen acceder a la red de Internet deben tener un rango de direcciones públicas asignadas, estas direcciones son administradas por la autoridad de números asignados a Internet o mejor conocido como IANA.
Esta entidad dividió la administración por regiones en el mundo denominándoles RIR o registros regionales de Internet, en la figura 21 se muestra la distribución de estas empresas en el mundo.

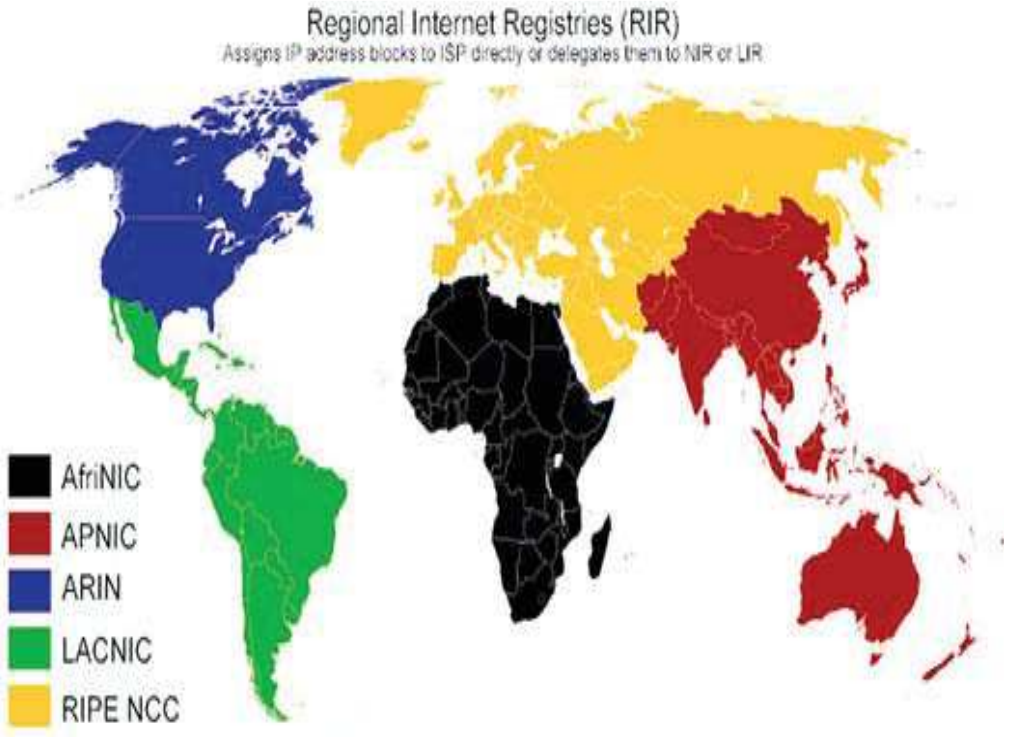


Figura 21. Distribución RIR en el mundo
Tomado de Cisco Networking Academy, 2013

Hoy en día los dispositivos electrónicos son creados con la finalidad de ser controlados y monitoreados, encontrando en IP el protocolo que ayuda a realizar este trabajo, razón por la cual estos aparatos necesitan de un identificador único en la red y debido a la masificación de esta tecnología la cantidad de direcciones IPv4 se está acabando de forma acelerada.

Es necesario indicar que de las 4294.967296 direcciones posibles solo se pueden hacer uso de 3700 millones de direcciones debido a los distintos tipos de direcciones que existe.

En la figura 22 se muestra las estadísticas del número de direcciones IP disponibles al 7 de septiembre de 2013, se dice que cuando se llegue por debajo de las 4. 194304 direcciones IPv4 todos los planes para evitar que las direcciones IPv4 se agoten quedarán en nada y será hora de pensar en la transición hacia un nuevo protocolo de direccionamiento.

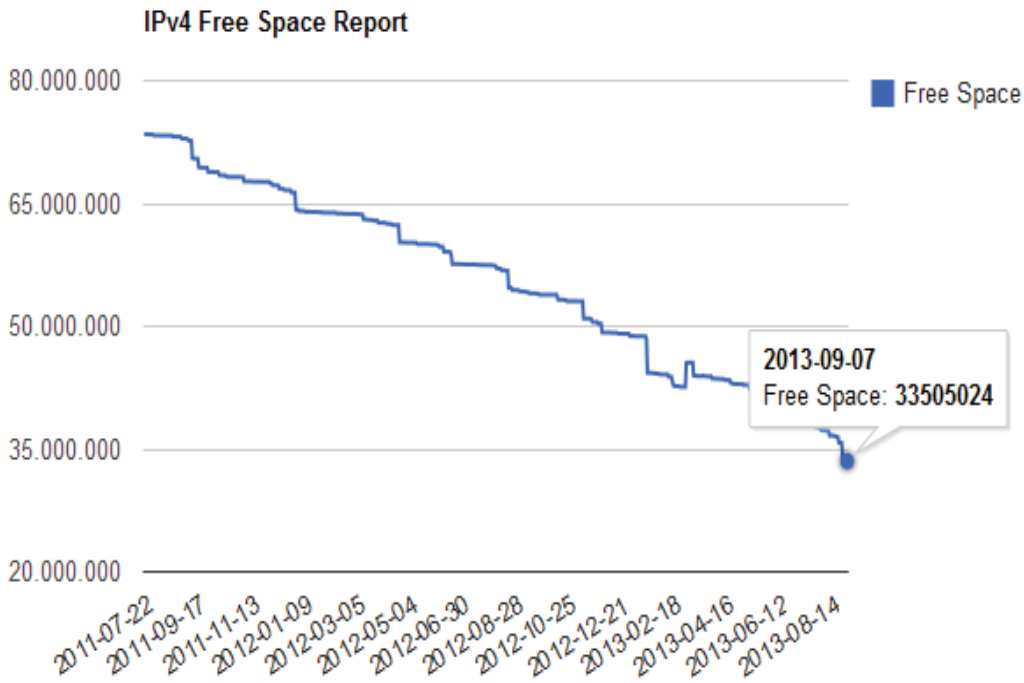


Figura 22. Reporte de espacio disponible de direcciones IPv4
Tomado http://www.lacnic.net/web/lacnic/reporte-direcciones-ipv4, 2013

Para ayudar al problema presentado se desarrollaron algunas alternativas de forma temporal como la asignación de direcciones privadas en redes locales y la traducción de direcciones conocido como NAT.

1.9.11 Uso de direcciones IPv4 de tipo privado

Dentro de las empresas, hoy en día es muy común observar que se hace uso de la tecnología para sus procesos de producción, a pesar de que la técnica TCP/IPes conocida en el uso de Internet, es preciso indicar que estos métodos de identificación de equipos también se los utiliza cuando se recurre a programas o aplicaciones que se sirvan de una red.

La asignación y administración del direccionamiento IPv4 dentro de las empresas pasa a ser responsabilidad única de cada una de ellas, los rangos de direcciones de tipo privado fueron ya mencionados en el direccionamiento IPv4, cabe indicar que para hacer uso de las direcciones de tipo privadas no se necesita que intervenga ninguna entidad de registro de direcciones IP.

La RFC 1918 diferencia a las máquinas que utilizan IPv4 en tres categorías:

- Categoría 1.- Máquinas que precisan de un direccionamiento único y que no necesitan intercomunicarse con otras redes.
- Categoría 2.- Maquinas que necesitan utilizar servicios específicos de Internet como telnet, ftp, correo electrónico.
- Categoría 3.- Máquinas que necesitan de acceso a internet, por lo tanto exigen un direccionamiento único.
- El uso de direccionamiento de tipo privado nos permite identificar algunos beneficios como:
- Utilizar direcciones públicas solamente en caso de ser necesario mostrarse en Internet.
- Permitir que las redes de las empresas se vuelvan totalmente flexibles, ya que al utilizar direccionamiento privado podrán hacer uso de más direcciones IP.

1.9.12 NAT (Network addresstraslation)

Otro de los métodos para evitar el agotamiento de direcciones IPv4 es utilizar la traslación de direcciones desde una red interna hacia Internet, esto con el fin de que las empresas puedan direccionar todos sus hosts con direcciones de tipo privado y utilizan NAT para salir a Internet.

La forma como realiza la traslación de direcciones IPv4 es mediante un equipo de borde que ejecuta un software especializado (NAT), este permite aumentar la privacidad de la red al ocultar las direcciones IP de la red interna.

El enrutador es el equipo que se utiliza como borde para que un hosts desde una red interna pueda realizar un transmisión a un host en el exterior, usualmente este dispositivo llega a ser la puerta de enlace para todos los hosts de un red interna, para NAT la red interna es el conjunto de redes que están sujetos a traducción.

Vamos a definir algunos términos utilizados por NAT:

Dirección local interna: Se considera a toda aquella única dirección IPv4 asignada a un host.

Dirección global interna: Se considera una dirección de red que contiene a un grupo de direcciones IPv4 locales.

Dirección local externa: Considerada como la IP que permite acceder a Internet en donde se enmascaran las direcciones de la red interna.

Dirección global externa: Considerada como una dirección de red que contiene a un grupo de direcciones IPv4 públicas.

1.9.12.1 Tipos de NAT

- NAT estático: Este tipo de NAT fue diseñado para que cada una de las direcciones IP de una red interna se asigne a su correspondiente dirección pública, con el fin de que puedan ser accesibles desde Internet, usualmente los servicios que se publican son DNS, FTP, HTTP.

En la figura 23, se muestra lo expuesto:

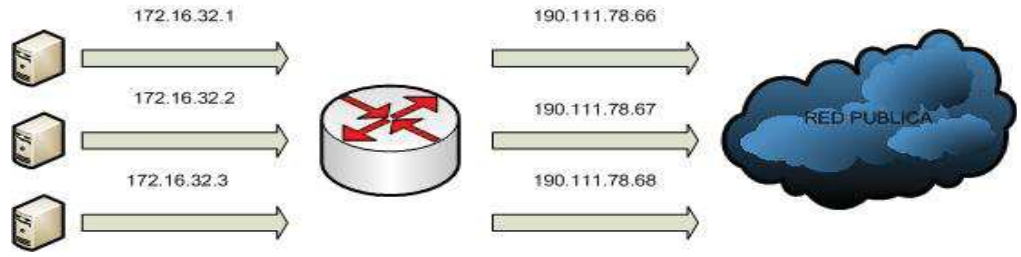


Figura 23. NAT estático
Tomado de Cisco Networking Academy, 2013

- NAT dinámico: Este tipo de NAT utiliza un grupo de direcciones IPs privadas que serán redireccionadas a un grupo de direcciones IP públicas de forma de forma dinámica, es decir que los equipos de una red interna podrán utilizar cualquier dirección IP pública que esté disponible.

En la figura 24, se muestra lo expuesto:

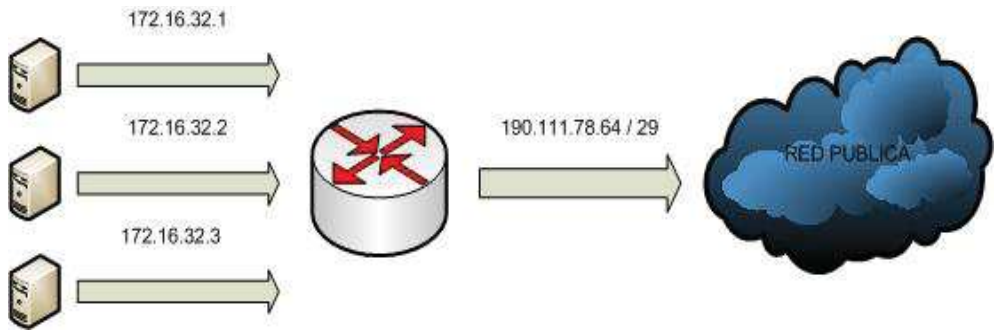


*Figura 24.*NAT dinámico
Tomado de Cisco Networking Academy, 2013

- NAT con sobrecarga: Esta característica de NAT es la más utilizada ya que recurre a una única dirección IP pública para redireccionar a varias direcciones IP privadas, para realizar este trabajo el enrutador hace uso de los puertos, existen 65.536 puertos para establecer conexiones.

En la figura 25, se observa el funcionamiento de NAT con sobrecarga.

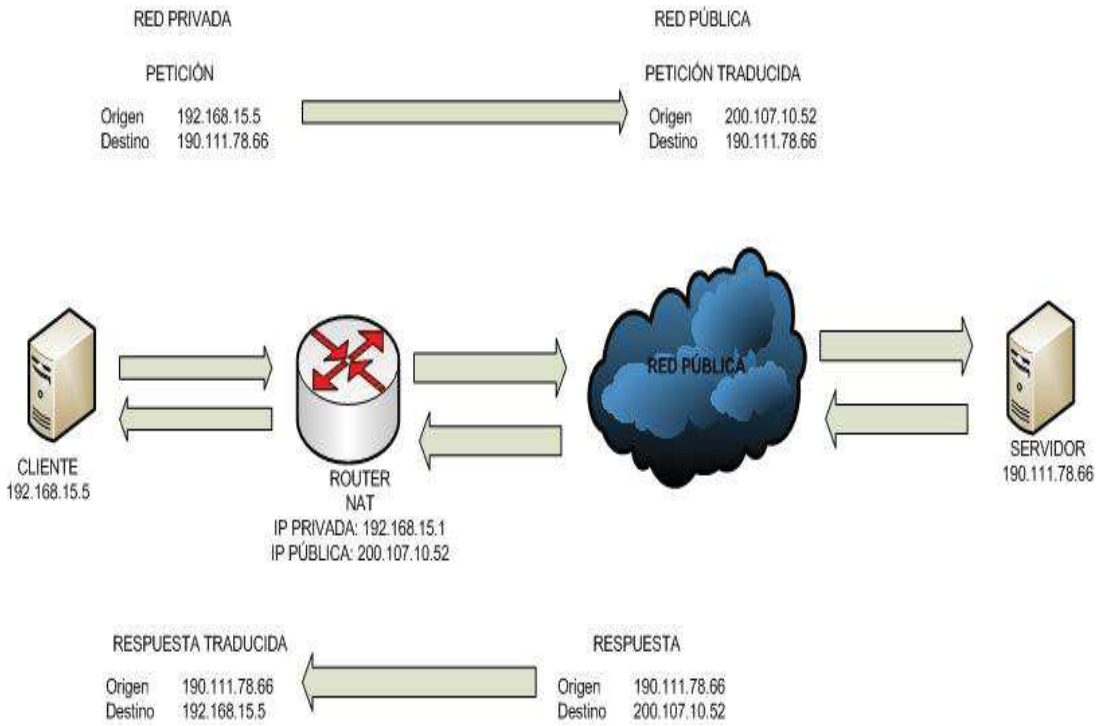


*Figura 25.*NAT con sobrecarga
Tomado de Cisco Networking Academy, 2013

1.10 IPv6

1.10.1 Introducción

Cada vez que un equipo necesita acceder a los servicios de Internet este debe utilizar un identificador único conocido como dirección IP, como ya hemos

anticipado en el análisis del protocolo de Internet versión 4 las direcciones de tipo público en el mundo cada vez van terminando.

El grupo de ingeniería de Internet o mejor conocido como IETF, preocupado por el agotamiento acelerado de direcciones IPv4, desarrolló un nuevo protocolo denominado IPv6 considerando algunos tópicos para su propuesta como el manejo mejorado de paquetes, escalabilidad y longevidad mejorada, calidad de servicio.

En el desarrollo de este protocolo se tomaron en cuenta los niveles de seguridad que se deberían integrar, es así que a IPv6 le agregaron algunas características en su diseño, detalladas de la siguiente forma:

- Fue diseñado con un direccionamiento jerárquico de 128 bits con el fin de poder obtener un direccionamiento bastante amplio, el número de direcciones IP que alcanzaría es de 670 mil billones de direcciones IPv6.
- Para optimizar el manejo de paquetes realiza la simplificación del formato del encabezado.
- Es escalable y el manejo de paquete lo realiza de mejor manera realizando un soporte mejorado para extensiones y opciones.
- Tiene capacidad de manejar calidad de servicio.
- Integra mejor la seguridad a través de autentificación y privacidad.

1.10.2 Formato del encabezado IPv6

En la figura 26, se muestra la composición del encabezado del protocolo IPv6.

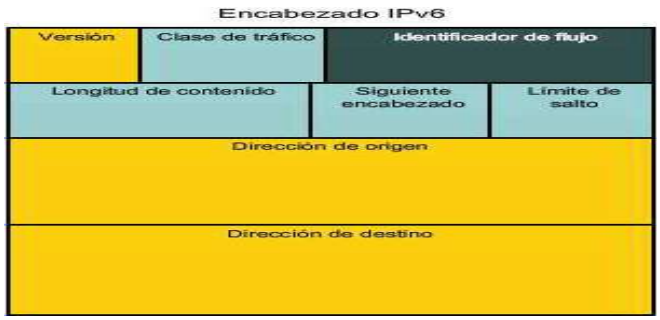


*Figura 26.*Encabezado IPv6

Tomado de Cisco Networking Academy, 2013¡

Cada uno de los campos va a ser descritos a continuación:

Versión: Protocolo de Internet de 4 bits, número 6.

Clase de tráfico: Campo clase de tráfico de 8 bits

Identificador de flujo: Identificador de flujo de 20 bits.

Longitud de contenido: Entero sin signo de 16 bits. Longitud de la carga útil IPv6, es decir, el resto del paquete que sigue a esta cabecera IPv6, en octetos.

Siguiente encabezado: Selector de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera IPv6.

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

Dirección de origen: Dirección de 128 bits del originador del paquete.

Dirección de destino: Dirección de 128 bits del recipiente pretendido del paquete. La Sociedad Internet (1998).

1.10.3 Direccionamiento IPv6

El siguiente tema que analizará es la arquitectura de direccionamiento, espacio de direcciones, formato de la dirección y la forma como se asignará una dirección a un equipo.

La RFC 3513 cuyo enfoque es la arquitectura de direccionamiento de IP versión 6 definen tres tipos de direcciones: únicast, multicast y anycast.

1.10.3.1 Direcciones unicast

Se utilizan para comunicaciones host a host.
Pueden ser sumarizadas, para esto las direcciones son acompañadas por un prefijo que especifica una cantidad determinada de bits significativos.

1.10.3.1.1 Direcciones globales

Son utilizadas para tráfico global y tienen una estructura jerárquica de 3 niveles:

- Un prefijo de enrutamiento global (red), típicamente de 48 bits.
- Un identificador de enrutamiento local (subred), de 16 bits.
- Un identificador de interfaz de 64 bits de longitud.

La longitud de cada porción es arbitraria, pero generalmente se respetan los 64 bits del ID de interfaz para mantener compatibilidad con múltiples implementaciones.

En la actualidad IANA y RIR están asignando direcciones del rango 2000::/3.

1.10.3.1.2 Direcciones unique local

Son direcciones que tienen el alcance de un sitio específico sin garantías de que sean globalmente únicas. Estas direcciones tienen una estructura propia:

- Un prefijo FC00::/7 de 8 bits.
- Un ID global pseudo-aleatorio de 40 bits.
- Un ID de subred de 16 bits.
- Un identificador de interfaz de 64 bits.

Estas direcciones no son enrutables sobre Internet.

1.10.3.1.3 Direcciones link-local

Todas las interfaces que operan con IPv6 tienen una dirección link-local. Su alcance está limitado al enlace y no son reenviadas. Son generadas dinámicamente con el prefijo FE80: /10 y un identificador de interfaz de 64 bits.

Permiten la comunicación entre dispositivos que están en un mismo segmento de red sin necesidad de otro tipo de direcciones. Se utilizan en procesos de configuración automática, descubrimiento de vecinos y descubrimiento de enrutadores.

1.10.3.1.4 Direcciones para propósitos especiales

Dirección sin especificar:::
Se utiliza como dirección de origen con propósitos especiales, por ejemplo en solicitudes DHCP.

Nunca ocupa el campo de dirección de origen en un encabezado IPv6. Si así fuera el paquete no será reenviado.

Dirección de loopback: ::1
Como en el caso de la dirección 127.0.0.1, define una interfaz local para el stack IP.

1.10.3.2 Direcciones Multicast

Es una dirección para un conjunto de interfaces. Cuando un paquete se envía a una dirección multicast este es recibido por todos los equipos que conforman la red.

1.10.3.3 Direcciones Anycast

Es una dirección que se configura a un grupo de interfaces, en este caso cuando se envía un paquete a esta dirección será recibo por el equipo más cercano en la red.

En IPv6 la dirección de broadcast ya no es tomada en cuenta encargando sus funciones a las direcciones de anycast y multicast.

1.10.3.4 Representación de direcciones

Existen tres formas de representar direcciones IPv6 en su forma convencional:
La primera forma y más conocida es representando 8 grupos de caracteres hexadecimales separados por ":". En el siguiente ejemplo observaremos una dirección Ipv6 típica:

fe80:f4ca:3f24:b432:26d8:0000:0000:0023

Esta dirección está dividida en dos grupos la dirección de red y la dirección del equipo.

La dirección de red estará compuesta por:

fe80:f4ca:3f24:b432

La dirección de equipo estará compuesta por:

26d8:0000:0000:0023

La segunda forma se refiere a la representación de una dirección cuando está compuesta por cadenas de ceros, considerando que los ceros a la izquierda son suprimidos, y se los muestra en el siguiente ejemplo:

fe80:f4ca:3f24:b432:26d8::23

La tercera forma de representar una dirección se refiere cuando se quiere utilizar un sistema hibrido de nodos Ipv4 e Ipv6, como se indica en el siguiente ejemplo: 0:0:0:0:0:0.12.2.69.4

1.10.3.5 Representación de prefijos de red

En el protocolo IPv6 el prefijo de red está representado por un número decimal parecido a los prefijos de red de IPv4, para comprender de mejor manera lo mostraremos en la siguiente notación:

dirección-ipv6/longitud de prefijo

Dirección-ipv6: Es una dirección cualquiera IPv6, representada en las formas ya conocidas.

Longitud de prefijo: es un valor decimal con el que detalla cuantos de los bits más significativos, constituyen el prefijo de la dirección.

En el siguiente ejemplo mostraremos una dirección IPv6 con su prefijo de red:

fe80:f4ca:3f24:b432:26d8:0000:0000:0023 / 64

o

fe80:f4ca:3f24:b432:26d8::23 / 64

2. Situación actual

2.1 Introducción

Entre las atribuciones de la Secretaría de Hidrocarburos son las de suscribir, modificar y administrar áreas y contratos petroleros, adicionalmente realiza estudios sobre nuevos yacimientos hidrocarburíferos. Tomado de http://www.hidrocarburos.gob.ec/la-secretaria.

Por esta razón y con el fin de precautelar el funcionamiento de sus sistemas informáticos, se implementó una infraestructura de red basada en equipos de comunicación que les permita tener agilidad y seguridad en sus procesos.

En la figura 27, se muestra el modelo de red diseñado por la entidad.

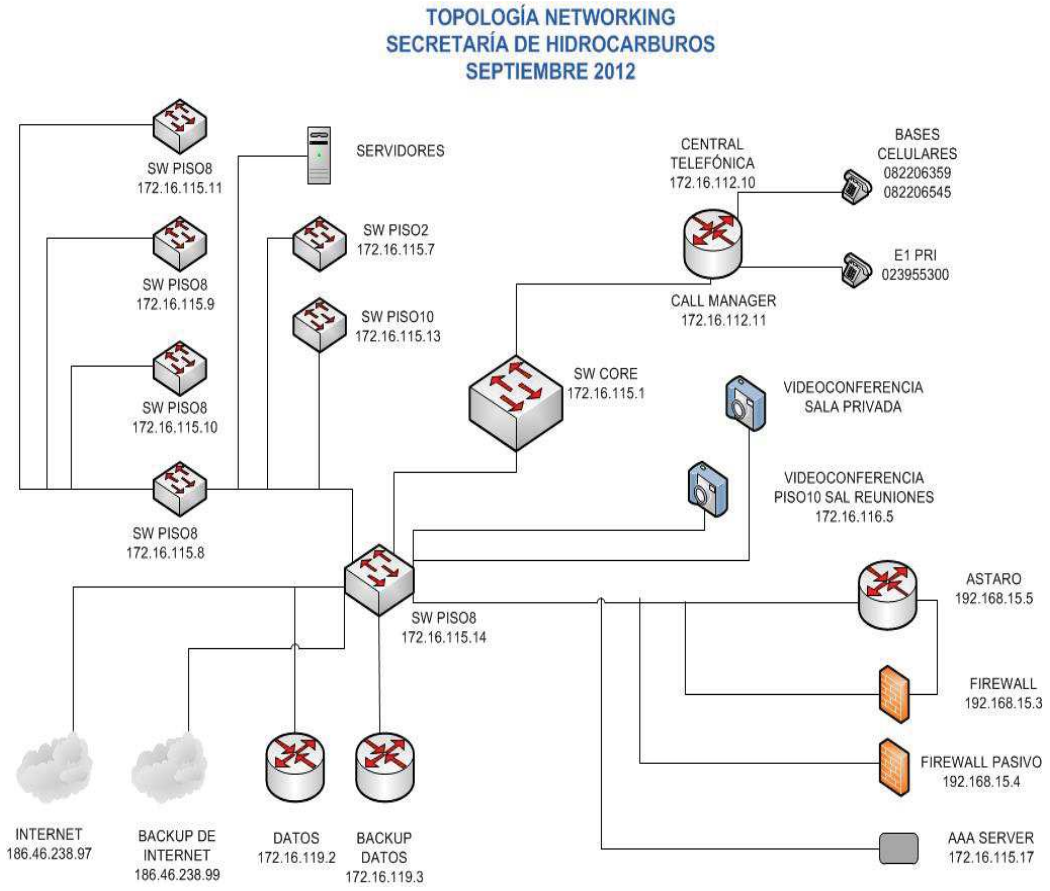


Figura 27. Topología de la red de la Secretaria de Hidrocarburos

2.2 Análisis de la infraestructura LAN

La red de la Secretaria de Hidrocarburos se basa en un modelo de red jerárquico en el que sobresale una estructura core y acceso. En lo que se refiere a servidores, su infraestructura se basa en la plataforma Microsoft, en el que el sistema operativo Windows Server 2008 resalta como herramienta de dominio activo, adicionalmente tienen configurado el servicio DHCP para la asignación de direcciones IP de forma dinámica, y el DNS para el reenvío de paquetes.

En la figura 28, se muestran los equipos instalados en el centro de datos en donde sobresale el rack de servidores, rack de networking y el rack de la central telefónica.

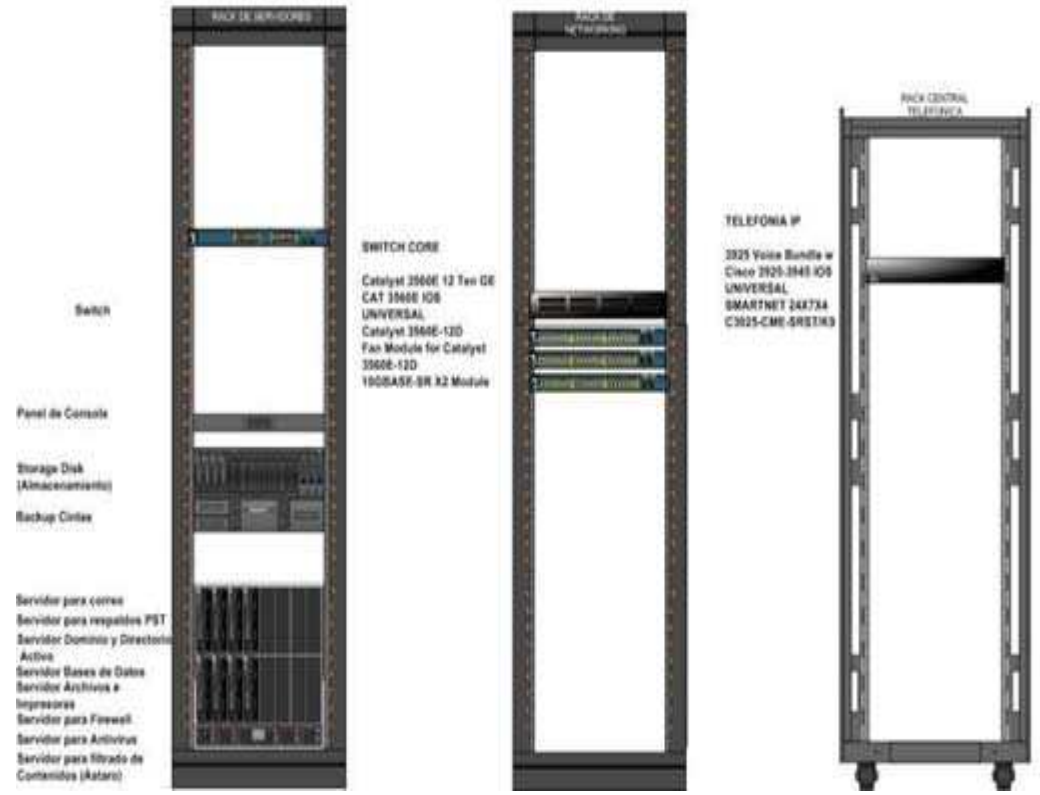


*Figura 28.*Diagrama de elevación de equipos de telecomunicaciones y servidores

De acuerdo a la figura 28, ahora se describirá a cada uno de los equipos que conforman la red de datos de la entidad.

El switch de core es un equipo Cisco Catalyst 3560-E series, este permite la conectividad únicamente a través de módulos para fibra óptica su interface es de tipo LC, los conectores LC fueron diseñados por la empresa Lucent Technologies en el año de 1997 y se los utiliza para conectar equipos de telecomunicaciones, circuitos cerrados de televisión y sistemas de telefonía, como característica especial de estos es que son pequeños, su arquitectura permite asegurar la conectividad y son fáciles de utilizar.

Al momento se encuentra habilitados dos puertos con interfaces para fibra óptica, el puerto número uno de este equipo permite conectar la estructura central de red o mejor conocido como backbone, admitiendo el enrutamiento y propagación de VLAN.

La comunicación con los equipos switch de acceso se lo realiza utilizando como medio de transmisión fibra óptica, la conectividad se la realiza al switch SW_DISP5_SHE ubicado en el rack de networking, en este equipo adicionalmente se conectan las interfaces configuradas como internas de los enrutadores de la red de datos e Internet entregado por la CNT, cabe indicar que en este switch tiene dos puertos de uplink de fibra óptica, identificados como número 25 este conecta al switch de core, el puerto número 26 realiza la conectividad con el switch SW_DISP3_SHE, este posee de igual forma dos puertos de uplink de fibra óptica identificados con el número 25 el mismo que se conecta con el switch anteriormente mencionado y el puerto numero número 26 se conecta mediante fibra óptica al puerto 26 del SW_DISP2_SHE.

La conectividad al SW_DISP7_SHE se las realiza mediante interface Ethernet utilizando como medio de transmisión al cable UTP cat 5e, de igual manera la conectividad al switch SW_DISP8_SHE es realizada mediante cable UTP Cat 5e.

Hay que considerar que para obtener el paso de VLANS desde el switch de core todos los puertos que se interconectan entre ellos deben estar configurados en modo trunk.

El puerto número dos delswitch de core tiene el módulo de fibra óptica instalado y permite la conectividad con el equipo enrutador de telefonía Cisco CME 3900 series.

Por otra parte,para la seguridad perimetralutilizan dos equipos Cisco ASA 5520 series en forma de principal y respaldo, las características más importantes se las muestra a continuación:

- Tráfico máximo de firewall hasta 450 Mbps.
- Conexiones máximas hasta 28000.
- Nueva conexión máxima en segundos hasta 12000.

Este equipo es el encargado de realizar la traslación de direcciones IP desde las IPs privadas hacia las IPs públicas, utilizando NAT para realizar el mencionado trabajo, este a su vez maneja las conexiones de usuarios remotos mediante conexiones VPN con formato de seguridad IPSec, hay que tomar en cuenta que una VPN es una conexión privada virtual que permite a los usuarios acceder a las aplicaciones que posee la entidad desde cualquier sitio donde tengan conexión a Internet.

Cuando un usuario necesita conectarse a la VPN debe tener un software de tipo cliente que le permita realizar esta conexión y un usuario que le permita autentificarse a la red VPN.

El equipo ASA 5520 de respaldo mantiene una configuración de espera, en caso que el equipo ASA principal presente algún inconveniente de tipo técnico, el dispositivo de respaldo pasa a realizar el trabajo del principal.

Otro de los equipos que conforman la infraestructura de red es el enrutador encargado de la voz sobre IP, este es un dispositivo Cisco Call Manager Express o más conocido por sus siglas CCME, tiene instalado un software que permite el tratamiento de llamadas y telefonía IP, desarrollado por Cisco.

La voz sobre IP se ha desarrollado día a día, permite optimizar los recursos de una red cableada como inalámbrica, su forma de trabajo es mediante la utilización de los estándares del protocolo de Internet, este tipo de telefonía es considerada como resistente, segura y escalable.

Optimiza los recursos de red al convertir los teléfonos IP en switch admitiendo que en un área de trabajo necesite únicamente de una conexión de red, logrando la conectividad no solo del teléfono IP sino que también de otros dispositivos de red.

Este tipo de telefonía se conforma por el gateway que es el equipo que realiza la conversión de señales análogas a paquetes IP y viceversa, en algunos casos este trabajo ya no resulta necesario debido a que la PSTN también ha ido evolucionando, siendo a ahora las troncales SIP y E1 PRI las más utilizadas, y dentro de su tecnología se usan señales digitales y telefonía IP.

Otro de los equipos con los que trabaja este sistema de telefonía es el gatekeeper, este nos permite realizar el enrutamiento de señales, contiene los buzones de voz y el sistema de contestadora automática o mejor conocido como IVR.

Utiliza a SCCP como un protocolo de comunicaciones para la señalización de parámetros de hardware del sistema tales como teléfonos IP H323, Media Gateway Control Protocol, el protocolo SIP es también utilizado por este sistema para vincular terminales que se comunican a través de este protocolo, usado además para endosar la señalización de las llamadas a los Gateway.

Los equipos que se conectan al CCME son teléfonos de la familia Cisco 7911 y 7965G, se comunican a través del protocolo H323, estos dispositivos nos permiten hacer y recibir llamadas de tipo interno y comunicarse con la PSTN mediante códec G711ulaw, G711alaw.

La entidad tiene otro tipo de teléfonos como el Cisco Small Business SPA 303, estos equipos se comunican al enrutador de telefonía mediante el protocolo SIP y el puerto 5060, estos dispositivos realizan las mismas funciones que los teléfonos mencionados anteriormente.

En la figura 29, se muestra cómo se encuentran conectados los equipos de la red telefónica, cabe recalcar que los teléfonos se autentifican al CME 3900 series a través de una vlan de voz configurada en cada uno de los puertos de los switchs.

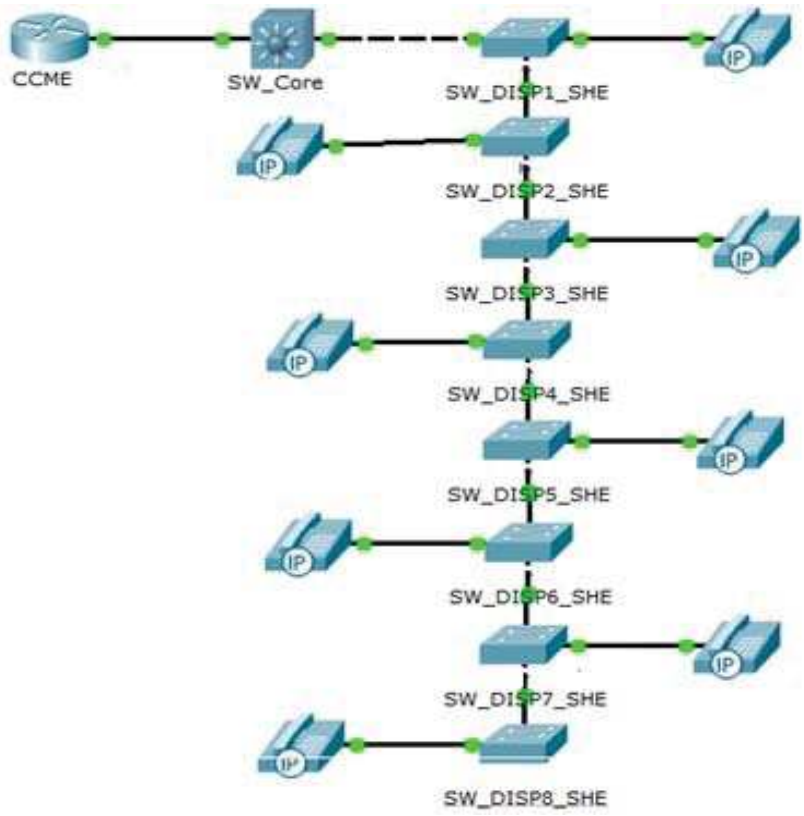


Figura 29. Topología de la red de telefonía IP

La seguridad interna de la red es administrada mediante un equipo Cisco 1121 Secure Access Control System, este dispositivo nos permite administrar los usuarios que podrán realizar la gestión de administración de red de acuerdo a los perfiles de usuario asignados, el tipo de seguridad que esta implementada es mediante TACACS+.

El ACS es un equipo que permite autentificar los equipos activos de red mediante un usuario y contraseña, una vez que se los registra en este sistema los equipos pasan a tener la misma forma de acceso permitiendo mejorar la administración.

La asignación automática de direcciones IP o mejor conocido como servicio DHCP, lo ejecuta un equipo servidor en el que se encuentra instalado el sistema operativo Windows 2008 server, en este se encuentra configurados los diferentes grupos de direcciones de acuerdo a lo indicado en la figura 30.

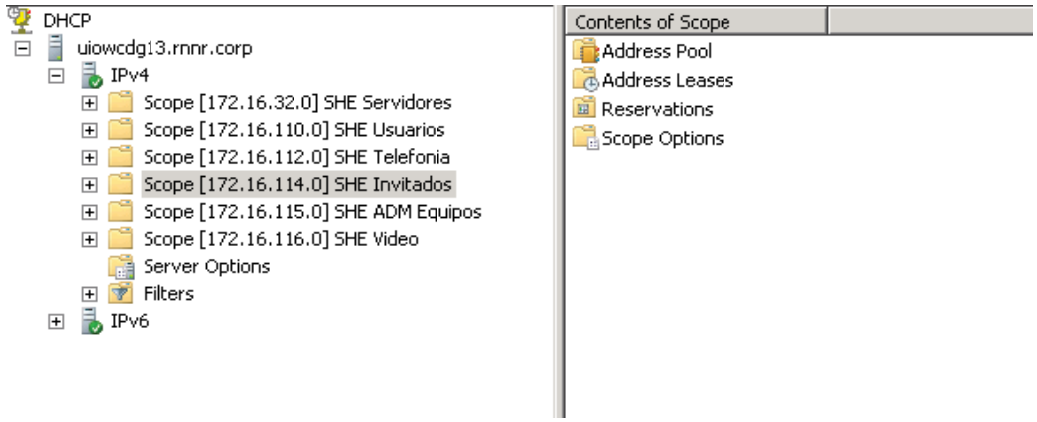


Figura 30. Grupo de direcciones DHCP

La función del servidor DHCP es la de entregar direccione IPv4 de forma automática a los equipos clientes de la red.

2.3 Análisis de la infraestructura WAN

En lo referente a la conectividad WAN, este servicio los provee la CNT, físicamente la entidad se conecta al proveedor mediante fibra óptica tanto en el enlace principal como el de respaldo.

El direccionamiento entregado por el proveedor es IPv4, la red asignada por ellos es la 186.46.238.96 con mascara 255.255.255.240, las mismas que están distribuidas de acuerdo a las necesidades de la entidad.

Las conexiones a las oficinas remotas se realiza por intermedio del proveedor CNT el mismo que entrega la conectividad en un equipo enrutador Cisco su direccionamiento es IPv4, este equipo se conecta mediante un cable de red UTP al puerto 24 y 14 del switch SW_DISP5_SHE configurado en la VLAN11 de datos.
En la figura 31 se muestra la forma como están conectados estos equipos.

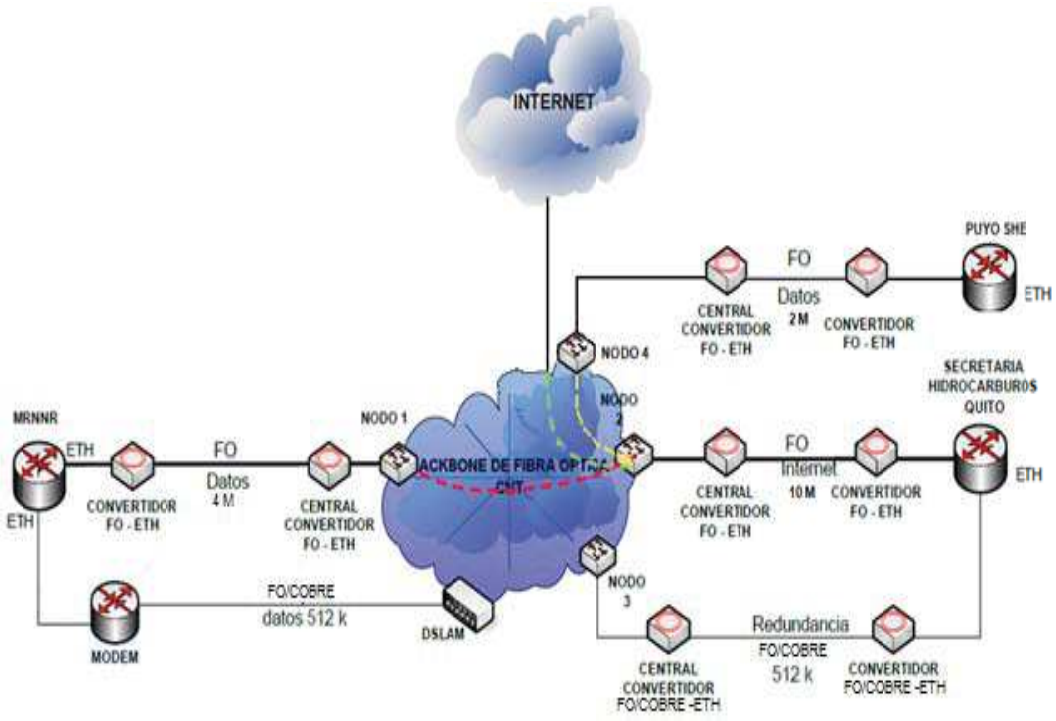


Figura 31. Red Wan Secretaría de Hidrocarburos

Como se observa en la figura 31, la CNT provee los servicios de Internet y transmisión de datos, utilizan convertidores para transformar el medio de señales eléctricas a señale ópticas y viceversa, para luego conectarse mediante patchcord UTP a los equipos enrutadores tanto principal como de respaldo, posterior a esto se enlaza al switch SW_DISP5_SHE de la entidad.
Para la segmentación de datos estos enlaces se conectan a la vlan 8 que está asignada para la conectividad de los equipos de Internet tanto de las interfaces de salida de los equipos ASA como de la interface LAN de equipo enrutador de Internet que provee la CNT.

2.4 Parámetros de la red LAN

Los parámetros de conectividad que tiene que tiene la red LAN de la entidad se basa en direcciones IPv4 de tipo privado. Para la asignación del direccionamiento tomaron en cuenta las VLAN que genera el equiposwitch de core, debido a esto en la tabla 6 se muestra las diferentes VLAN creadas y su parámetros de asignación de direccionamiento.

Tabla 6.VLANS configuradas en el switch de core

VLAN	Nombre	Dirección IP de interfaz	Máscara
2	SERVIDORES	172.16.32.1	255.255.255.0
3	USUARIOS	172.16.110.1	255.255.254.0
4	TELEFONIA	172.16.112.1	255.255.254.0
5	INVITADOS	172.16.114.1	255.255.255.0
6	ADMINISTRACION	172.16.115.1	255.255.255.0
7	VIDEO	172.16.116.1	255.255.255.0
8	VLAN_OUTSIDE_CNT_INTERNET		
9	VLAN_ASA_INSIDE	192.168.15.3	255.255.255.0
10	VLAN_ASA_FAILOVER		
11	VLAN_ENLACE_MRNNR	172.16.118.1	255.255.255.0

Las VLANs que se muestran en la tabla 6 son propagadas mediante el protocolo VTP siendo este importante en la administración de la red, ya que este nos permite de una manera centralizada realizar cambios en las configuración de las VLANs en el equipo core y en cuestión de 300 segundos estos cambios son actualizados de forma automática en los equipos switches de acceso clientes de VTP.

Como dice Creative Commons The Evangelist INFO (2004 - 2013). “VTP es un protocolo que usa tramas de la capa de acceso para distribuir información de VLANs entre los switches.”

2.5 Parámetros de la red WAN

Los parámetros de conectividad que tiene que tiene la red WAN de la entidad se basa en direcciones IPv4 de tipo privado para la red de datos, y para la conectividad de Internet la CNT asignó un grupo de direcciones IPv4 de tipo público.

En la figura 32, se muestran los parámetros de la red WAN en donde se puede observar las IPs de tipo público para Internet y las IPs de tipo privado para la red de datos.

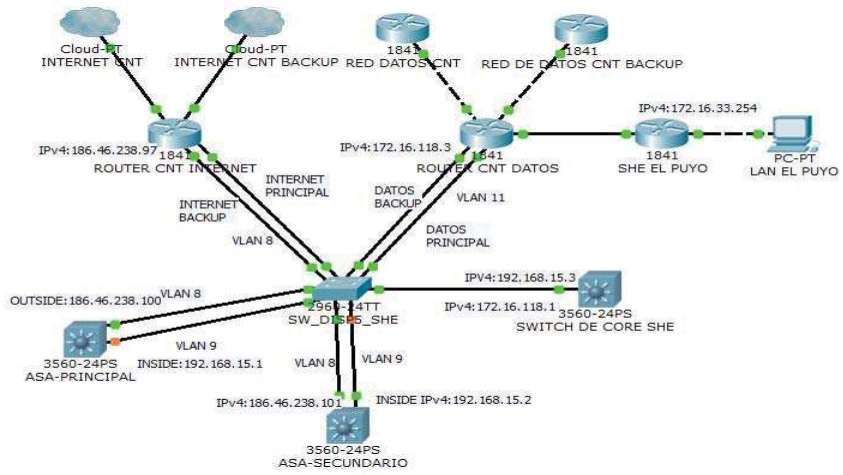


Figura 32. Parámetros de la red WAN

2.6 Razones para remplazar el direccionamiento IPv4

El continuo desarrollo de la tecnología y la demanda masiva de acceso a Internet en el mundo nos ha llevado a que el direccionamiento a través del protocolo IPV4 sea cada vez más escaso, razón por la cual se debe buscar un proceso de migración que permita utilizar un protocolo que maneje un direccionamiento IP más extenso.

En la entidad se ha visto necesario realizar estudios, para evaluar la situación actual de los equipos de telecomunicaciones y que permita migrar hacia un nuevo protocolo de red y direccionamiento.

Adicionalmente se debe considerar que debido a las necesidades institucionales se ha incrementado los equipos tecnológicos y que para la adquisición de estos se debe tomar en cuenta que estos soporten nuevas tecnologías tanto en protocolos como direccionamiento.

Como información adicional es posible indicar que en el Acuerdo-No.-039-2012 del Ministerio de Telecomunicaciones de Ecuador, consideran como política del estado ecuatoriano, para las entidades públicas y privadas, realizar los análisis necesarios para interactuar con el protocolo IPV6 tanto a nivel LAN como WAN.

3. Desarrollo de la propuesta

3.1 Introducción

La Internet ha sido siempre una red multiprotocolo, a su vez esta se encarga de transportar paquetes a través de una variedad de redes. En este capítulo se analizarán los diferentes escenarios de migración y transición propuestos por la IETF y RFCs. Las técnicas de migración que se presentarán serán consideradas como buenas prácticas y podrán ser adoptadas por administradores de red que sientan la necesidad de adoptar el protocolo IPv6.

3.2 Actualización a un nuevo protocolo

Para ejecutar el proceso de migración de un protocolo IPv4 a un protocolo IPv6 se debe tomar en cuenta lo siguiente:

- Los ingenieros a cargo del proceso de migración deberán realizar una demostración con software de simulación de redes como Packet Tracert o GNS3 de tal manera que se pueda probar las configuraciones deseadas.
- Los ingenieros a realizar este proceso de migración deberán estar en la capacidad de conocer las características y beneficios que ofrece IPv6.
- Modificar la configuración de DNS de tal forma que soporte direcciones IPv6.
- Configurar IPv6 en la infraestructura de la red de datos, verificando que tanto equipos servidores y clientes soporten el protocolo propuesto.
- Se deberá utilizar necesariamente de forma simultánea los protocolos IPv4 e IPv6, con el fin de seguir utilizando los sistemas existentes.
- Los especialistas en desarrollo de software tienen que tomar en cuenta que las futuras aplicaciones que se generen deberán soportar el protocolo IPv6.

3.3 Técnicas de migración

Existen algunas herramientas disponibles para realizar este proceso de migración, las mismas que ayudarán a soportar IPv6 fácilmente, entre ellas citaremos las siguientes:

- Conexión nativa IPv6
- Conectividad IPv6 basada en túneles
- Túneles automáticos (6to4)
- Túneles automáticos intra-site (ISATAP)

3.3.1 Conexión nativa IPv6

Este es uno de los métodos de migración más simples que puede haber, debido a que el direccionamiento de los equipos será exclusivamente IPv6, para lo cual se deberá utilizar una red con direccionamiento IPv6 con prefijo /48, para luego utilizar las subredes que se pueden generar en esta con prefijo /64.

3.3.2 Conectividad IPv6 basada en túneles

Túneles IPv6 es una técnica para establecer un camino virtual entre dos nodos IPv6 que servirá para transmitir paquetes de datos válidos. Desde el punto de vista de los dos nodos, este camino virtual es como una conexión punto a punto con dos actores IPv6 y trabajan en la capa de enlace de datos. Los dos nodos IPv6 cumplen roles específicos, el uno encapsula el paquete original recibido desde otro nodo y lo envía a través del túnel. El otro nodo desencapsula el paquete recibido por el túnel y retransmite el paquete original hacia su destino. El nodo encapsulador es llamado punto de entrada del túnel, siendo este el origen de los paquetes del túnel. El nodo desencapsulador es llamado el punto de salida del túnel y es este el destino de los paquetes del túnel.

Existen dos tipos de túneles entre ellos citaremos a los túneles manuales y a los túneles automáticos.

3.3.2.1 Túneles manuales

Tuéneles manuales son utilizados para construir conexiones que permitan que el tráfico IPv6 fluya a través de las redes IPv4, son fáciles de administrar, pero requieren de mucha atención debido a que se debe tener en cuenta la configuración de cada destino de red.

En la figura 33, se observa dos redes IPv6 en los segmentos LAN, dos enrutadores dual stack con una conectividad WAN IPv4.

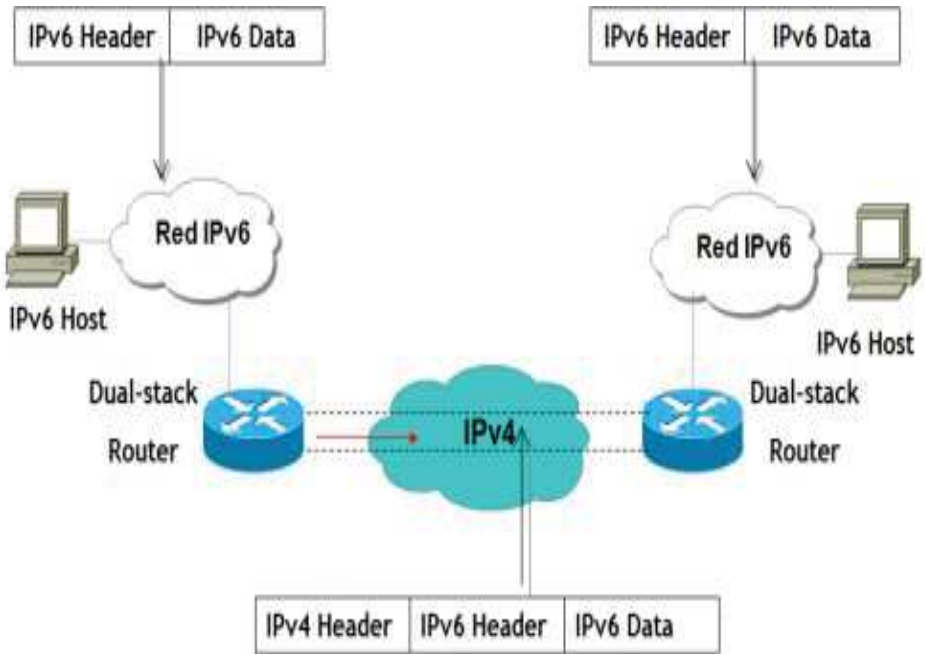


Figura 33. Túnel IPv6 con Dual Stack
Tomado de http://www.cu.ipv6tf.org/transicionipv6.htm, 2014

Para evitar estas configuraciones manuales se debe considerar otro tipo de soluciones como lo son los túneles automáticos.

3.3.2.2 Túnel GRE

Otro tipo de túnel manual es GRE, este fue desarrollado por Cisco permite transmitir paquetes de una red por una red diferente que puede ser de un proveedor de servicios de Internet, para este trabajo de titulación se tomará en cuenta este tipo de túnel para conectar las oficinas remotas que poseen direccionamiento IPv6.

Se considera una desventaja utilizar este tipo de túneles la necesidad de tener una configuración previa, adicionalmente con este tipo de solución no es posible detectar la caída de un enlace.

La RFC 1701 específica a GRE y realiza algunas recomendaciones al respecto de este tipo de túnel, en la figura 34, se muestra la forma que debe tener el paquete encapsulado.

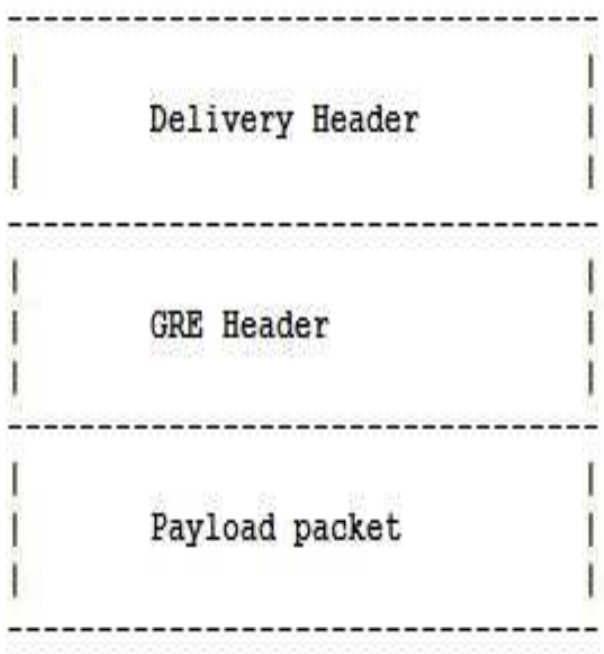


Figura 34. Encabezado de paquete GRE
Tomado de http://tools.ietf.org/html/rfc1701, 2014

En la figura 35, se observa cómo está compuesto el encabezado del paquete.

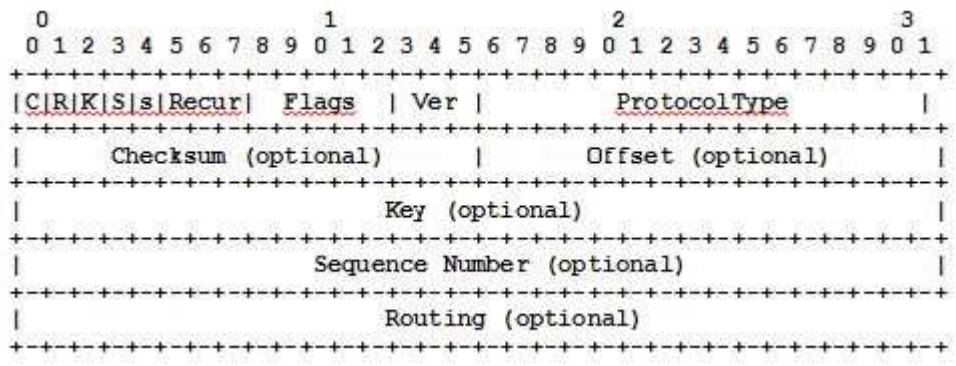


Figura 35. Encabezado de paquete GRE
Tomado de http://tools.ietf.org/html/rfc1701, 2014

Los campos como flag, Ver y Protocol Type pasan a ser los más importantes del encabezado de paquete ya que contiene información como tipo de protocolo, codificación y la versión de campo.

En la figura 36, se verifica la manera como trabaja este túnel, con la interface de origen, IP destino en este caso la dirección es IPv4 y dentro del túnel se tendrá que configurar una dirección IPV6, adicionalmente se añade una cabecera de tipo GRE.

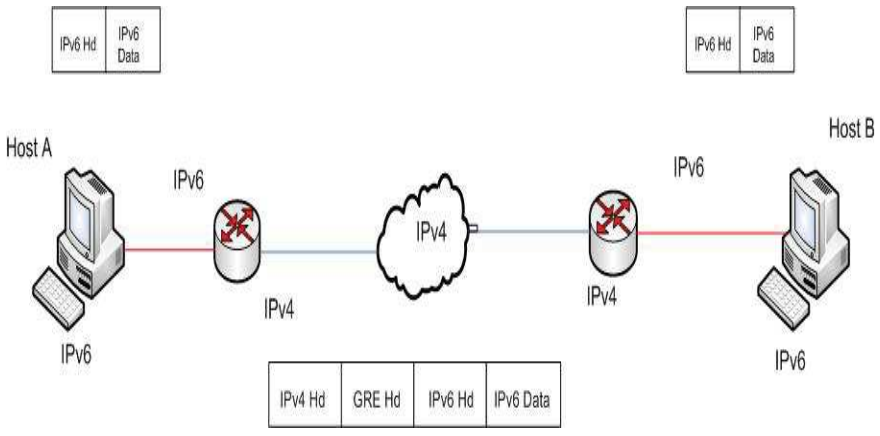


Figura 36. Funcionamiento túnel GRE
Tomado de Cisco Networking Academy, 2014

La forma como se envía los paquete es la siguiente el Host A enviará información de tipo IPv6 hacia su enrutador este le añadirá una cabecera de tipo IPv4 debido a que en el momento que se configura el túnel tanto en dirección de origen como destino se lo hace con direcciones IPv4, de esta forma el paquete podrá ser transportado por una red IPv4, añadirá además una cabecera GRE identificando que por detrás hay una cabecera IPv6 y finamente el paquete IPv6, al momento que el paquete llega al enrutador que conecta el host B, este se encarga de eliminar la cabecera IPv4 y la cabecera GRE una vez que se realiza esta tarea los datos pasa a ser netamente IPv6 entregando la información al Host B.

Como características adicionales de este tipo de túnel es que sobre este se puede establecer políticas de enrutamiento, seguridad, trabajan con redes de alta velocidad y ofrece transmisión sucesiva de paquetes.

3.3.2.3 Túneles automáticos 6to4

Los túneles automáticos 6to4 permiten la conectividad a redes con direccionamiento nativo IPv6 a través de una infraestructura IPv4.

Un equipo con direccionamiento IPv6 puede usar 6to4 de dos formas que se las muestra a continuación:

- Equipo 6to4 a equipo 6to4.
- Red 6to4 a equipo con direccionamiento IPv6 nativo.

En la figura 37, se muestra dos equipos 6to4 conectados a través de una red IPv4

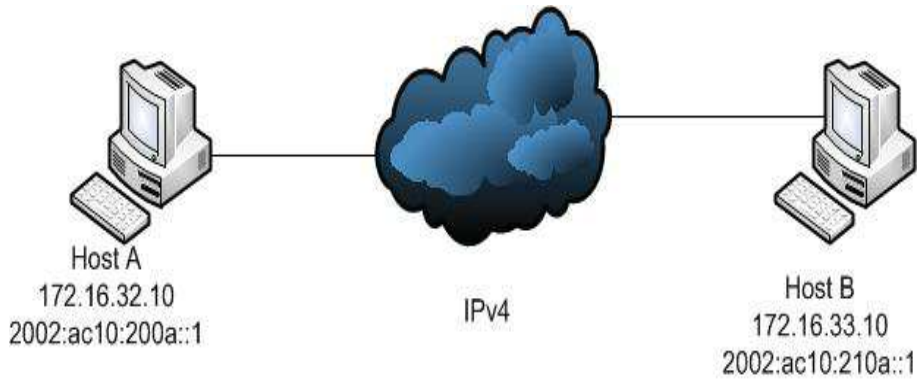


Figura 37. Túnel automático 6to4
Tomado de IPv6: Theory, Protocol and Practice, 2014

Como indica la figura 35 el host A tiene una dirección IPv4 172.16.32.10 y el host B tiene la dirección IPv4 172.16.33.10, la función de 6to4 es asignar bloques de direcciones IPv6 para estos equipos utilizando la dirección IPv4 como parte de la dirección y ubicándolos en el segundo y tercer grupo de identificadores hexadecimales puedan formar la nueva dirección IPv6.

En la figura 38, se muestra la estructura de una dirección 6to4.

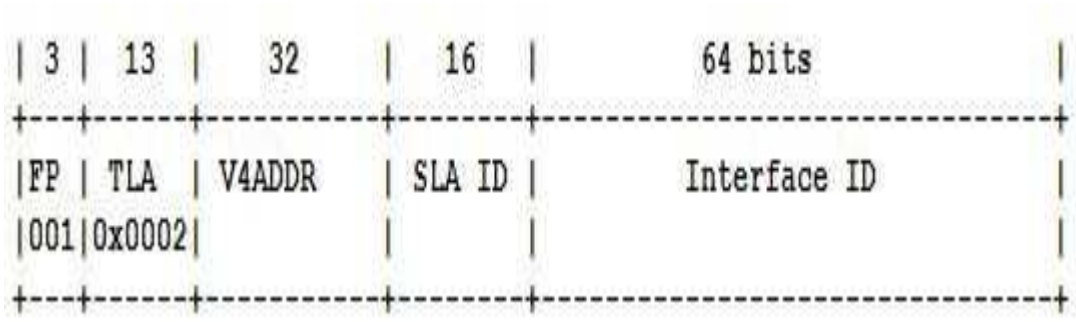


Figura 38. Estructura de una dirección IPv6 6to4
Tomado de RFC 3056, 2014

En donde:

- Los primeros 16 bits son FP y TLA forman el prefijo que indica que es una dirección 6to4, el número 2002 nunca cambia.
- Los siguientes 32 bits corresponde a V4ADDR y compone la dirección IPv4 expresada en formato hexadecimal.
- SLA ID está formado por 16 bits y corresponde al identificador de la subred 6to4.
- Los 64 bits restantes identifican al host el mismo que puede ser configurado de forma manual o utilizando un mecanismo de autoconfiguración.

En la tabla 7, se muestra la transformación de una dirección IPv4de su forma decimal a binaria y posteriormente a hexadecimal.

Tabla 7.Conversión de una dirección IPv4 a su formato hexadecimal

DECIMAL	BINARIO	HEXADECIMAL
172	10101100	AC
16	10000	10
32	100000	20
10	1010	A

Tomado de RFC 3056, 2014

Tomando como referencia la conversión de la dirección IPv4 172.16.32.10 tendremos la siguiente dirección 6to4.

2002:ac10:200a::/48

En la figura 39, se observa la encapsulación de un paquete IPv6 dentro de un paquete IPv4.

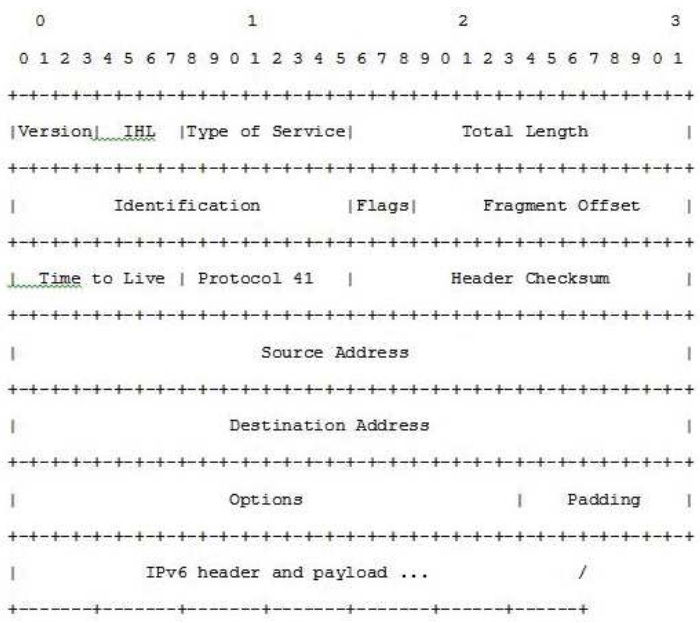


Figura 39. Encapsulación en IPv4
Tomado de RFC 3056, 2014

Como se puede observar los paquetes IPv6 son transmitidos en paquetes IPv4 haciendo referencia al protocolo 41, el mismo que especifica las formas de transmitir un paquete IPv6 sobre tramas IPv4, la cabecera IPv4 contiene el destino y las direcciones IPv4 de origen, adicional a esto el paquete IPv4 contiene la cabecera IPv6 y la carga útil.

En lo referente al funcionamiento de este túnel se diría que la configuración de este tipo de túneles usualmente se lo realiza en los enrutadores que permiten conectarse a redes remotas a través de un proveedor de servicios de internet, e este proceso los paquetes IPv6 al momento de ser transmitidos se lo encapsulan dentro de una trama IPv4 y se produce la acción contraria al momento que el paquete llega al enrutador de destino en este caso el paquete se desencapsula en el enrutador del proveedor de servicios de internet y entregará a su destino la red IPv6. FGV

3.3.2.4 Túneles automáticos ISATAP

ISATAP es una herramienta complementaria de transición que permite el transporte de paquetes IPv6 en una infraestructura donde el direccionamiento IPv6 nativo aún no está disponible, encapsulando paquetes IPv6 en encabezados IPv4, obteniendo que los hosts ISATAP puedan verse entre ellos usando IPv6 sobre una red IPv4.

Como característica de este tipo de túnel es que permite a los clientes se configuren de forma automática, utiliza un direccionamiento IPv6 con prefijo unicast /64 y un identificador de interfaz de 64 bits. El identificador de interfaz se crea en formato modificado EUI-64, siendo este un identificador de interface de 64 bits que se deriva usualmente de la dirección MAC de un dispositivo.

Los 64 bits indicados están compuestos por 32 bits que contienen el valor 0000:5EFE que identifican una dirección IPv6 ISATAP y los 32 bits siguientes son los conformados por la dirección IPv4.
En la tabla 8describe el formato de una dirección ISATAP.

Tabla 8.Formato de una dirección ISATAP

64 Bits	32 Bits ISATAP	32 Bits
Prefijo unicast IPv6, dirección local o global	0000:5EFE	Dirección IPv4 o enlace ISATAP

Tomado de http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/interface/configuration/xe-3s/ir-xe-3s-book/ip6-isatap-xe.html, 2014

Una vez que se ha revisado como está compuesta una dirección ISATAP, en la figura 40, se muestra como realiza su trabajo.

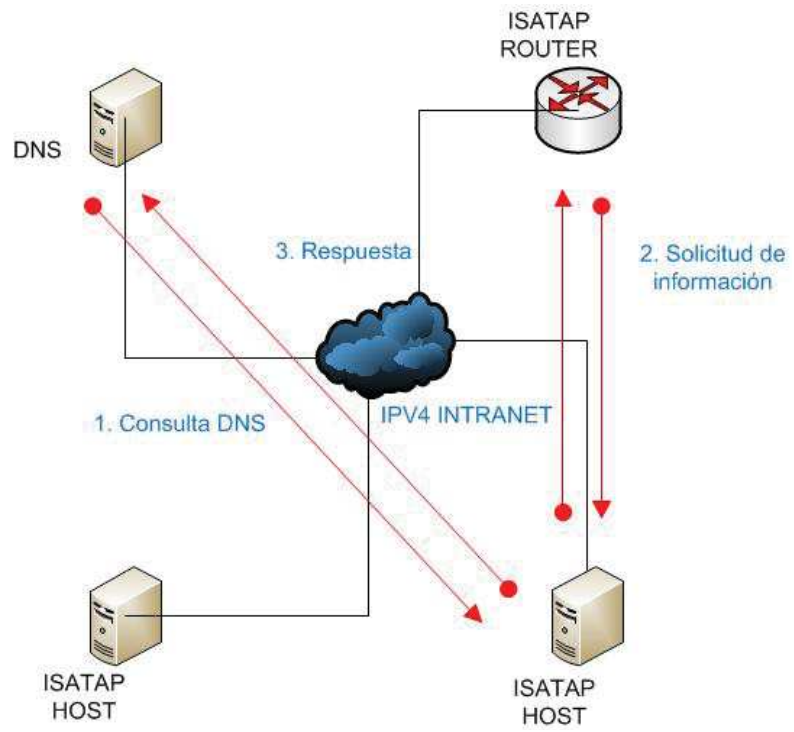


*Figura 40.*Funcionamiento ISATAP

Tomado de http://www.franciscosepulveda.eu/2011/12/08/tecnologias-de-transicion-a-ipv6-isatap-12/, 2014

La forma como realiza ISATAP la configuración automática de una interfaz de un host es la siguiente:

- El host ISATAP consulta al DNS buscando ISATAP, en este momento utiliza IPv4.
- Al momento que el host ISATAP realiza la consulta al servidor DNS le responde como resultado la dirección IP del enrutador ISATAP.
- La comunicación con el enrutador ISATAP se ejecuta utilizando tráfico IPv6 encapsulado en IPv4.

- El enrutador responde al host ISATAP sobre el prefijo que debe utilizar en la red y si el enrutador es la puerta de enlace.

3.4 Migrando hacia IPv6

El proceso de migración deberá ser necesariamente de forma gradual, debido a que las aplicaciones que aún trabajan con el protocolo IPv4 tendrán que seguir siendo utilizadas.

Como primera tarea vamos a reconocer los servicios con los que cuenta la entidad en su red LAN y que tendrán que necesariamente soportar la migración al protocolo IPv6.

3.4.1 Análisis de los servicios actuales

Los servicios que posee la Secretaría de Hidrocarburos y que deberán ser considerados al momento de realizar la migración al protocolo IPv6 se los detalla a continuación:

- Voz sobre IP
- Enrutadores
- Firewall
- Email
- DHCP
- Sistemas Operativos
- DNS
- Gestión de red
- Gestión de seguridad

De acuerdo a los servicios mencionados es necesario realizar un análisis del direccionamiento IPv6, el enrutamiento, y las formas de aplicar la seguridad.

3.4.2 Direccionamiento IPv6

En la tabla 9 se muestra el direccionamiento propuesto para los equipos de la red interna.

Tabla 9.Direccionamiento propuesto IPv6

VLAN	Nombre	Dirección IP de interfaz	Prefijo
2	SERVIDORES	2014:0:0:1::	64
3	USUARIOS	2014:0:0:2::	64
4	TELEFONIA	2014:0:0:3::	64
5	INVITADOS	2014:0:0:4::	64
6	ADMINISTRACION	2014:0:0:5::	64
7	VIDEO	2014:0:0:6::	64
8	VLAN_OUTSIDE_CNT_INTERNET		
9	VLAN_ASA_INSIDE	2014:0:0:7::	64
10	VLAN_ASA_FAILOVER		
11	VLAN_ENLACE_MRNNR	2014:0:0:8::	64

Como dice la IANA el grupo de direcciones IPv6 mínimo a asignar a las empresas que necesiten de este servicios es en bloques /48 del cual nos permite tener 65.535 redes /64, razón por la cual se plantea el direccionamiento descrito en la tabla 2.

En los grupos de direcciones IPv6 indicados se tiene un número de host disponibles por red de 18.446.744.073.709.551.615 direcciones unicast, al tener un direccionamiento extenso se hace posible que no existan límites de conectar tantos equipos como sean necesarios dentro de la red.

3.4.3 Direccionamiento estático

Este tipo de direccionamiento será configurado en equipos que por los servicios que prestan entre ellos DNS, Active Directory, aplicaciones, impresión deben

necesariamente tener IP fijas, para este caso se tomarán en cuenta a los servidores que se enlistan a continuación:

- Active Directory
- Impresión
- Aplicaciones
- Base de datos
- Video Vigilancia
- Respaldos

3.4.4 Direccionamiento de usuarios

Existen tres formas de configurar los equipos de los clientes entre ellas tenemos la forma manual que consiste en establecer de forma única una dirección IP en un host.

Otra de las formas es la autoconfiguración local, en este tipo de configuración un servidor DHCP envía a sus clientes información adicional del protocolo como DNS u otras configuraciones.

La tercera forma de asignar una dirección IP es conocida como estado completo es decir que las direcciones IPv6 las asignará un servidor DHCPv6 entregando toda la información adicional del protocolo como DNS, puerta de enlace y otros servicios que tenga habilitado.

3.4.5 Enrutamiento IPv6

Existen dos formas que permiten realizar el enrutamiento de paquetes al momento de utilizar IPv6, entre ellos mencionaremos al enrutamiento dinámico y enrutamiento estático.

En la figura 41, se muestra una ruta por defecto de IPv6, que sirve como guía para agregar cualquier ruta estática en IPv6, en donde vamos a señalar los siguientes campos:

Ipv6 route ::0/0 2014::2

*Figura 41.*Ejemplo de ruta estática

Tomado de Cisco Networking Academy, 2014

En donde:

IPv6 route:	Habilita el comando para agregar una ruta.
:: :	Todas las redes
/0 :	Cualquier prefijo
2014::2 :	Los paquetes se los enviará por el siguiente dispositivo conectado y utilizado como salida.

3.4.6 Enrutamiento dinámico

En lo que se refiere a enrutamiento dinámico con IPv6 tenemos tres protocolos que permiten la comunicación de esta forma entre ellos se mencionará a vector distancia o RIPNG, BGPv4 o mejor conocido como path vector, y a los protocolos de estado de enlace ISIS u OSPFv3.

Para el caso de este proyecto de titulación el enrutamiento en el equipo core se lo realizará de forma estática.

3.4.7 Servicios sobre IPv6

La infraestructura tecnológica de la Secretaría de Hidrocarburos por el momento se basa en la plataforma Microsoft Windows 2008 Server en servidores y Microsoft Windows 7 en sus clientes, razón por la que es

necesario listar los diferentes servicios que se podrán ejecutar sobre el direccionamiento IPv6.

- **Telnet**

  En una aplicación de tipo cliente-servidor como característica importante es que utiliza el puerto TCP 23 para establecer la comunicación, este servicio está incluido en los sistemas Windows se lo debe habilitar en los servicios.

- **SSH**

  Esta aplicación utiliza al puerto TCP 22 para establecer la comunicación entre equipos adicionalmente utiliza interfaces de comandos para su trabajo, este programa realiza su conexión segura debido a que utiliza un canal de comunicación con encriptación, en sistemas operativos Microsoft Windows esta aplicación debe ser instalada existiendo algunos gestores de esta aplicación como putty, xmanager, entre otros.

- **FTP**

  Es un protocolo que permite transferir archivos desde y hacia equipos remotos, utiliza los puertos 20 y 21, para esta labor en los sistemas Windows se utiliza algunos programas gestores de este protocolo como SolarWinds, Filezilla entre otros.

- **EMAIL**

  En este caso la plataforma de correo que utiliza la Secretaría de Hidrocarburos es el Microsoft Exchange Server, como dato importante es que el servicio SMTP soporta IPv6, por ende la herramienta puede ser configurada para utilizar el direccionamiento IPv6.

- **WEB**

  Los servicios web son soportados por IPv6 ya sea que se disponga de Apache o de Internet Información Server (IIS), estas aplicaciones utilizan el puerto de comunicaciones TCP 80 para comunicarse con sus clientes.

- **DNS**

  La función del DNS es la de traducir nombres de dominio en direccione IP que pueden ser IPv4, al momento la entidad tiene configurado y funcionando el servicio DNS para el protocolo IPv4.

  En IPv6 existen algunos cambios en relación a la forma de trabajar del DNS se crearon lo registros AAAA y los PTR sigue llamándose igual que en IPv4.

  Para el caso de infraestructura de la Secretaría de Hidrocarburos donde sus equipos DNS tienen instalado el sistema operativo Windows 2008 Server, al momento de agregar el servicio de DHCP automáticamente al momento de entregar direcciones de tipo IPv6 se asignan un nombre de tipo AAAA a estos equipos.

  Para el caso de los registros PTR o zona reversa deben ser creados de forma manual.

- **Registros AAAA**

  Los registros AAAA son utilizados por IPv6 para transformar nombres de dominio en direcciones IPv6, como característica adicional es que son de 128 bits.

- **Registros PTR**

  Al igual que en IPv4 los registros PTR son utilizados como un registro inverso, es decir que si un programa conoce la IP estos registros saben a qué dominio pertenece.

3.5 Diseño de la estrategia de migración técnica

En la figura 42, se muestra la estrategia técnica de migración que será utilizada para en la entidad tomando en cuenta dos escenarios que se los detalla de la siguiente manera.

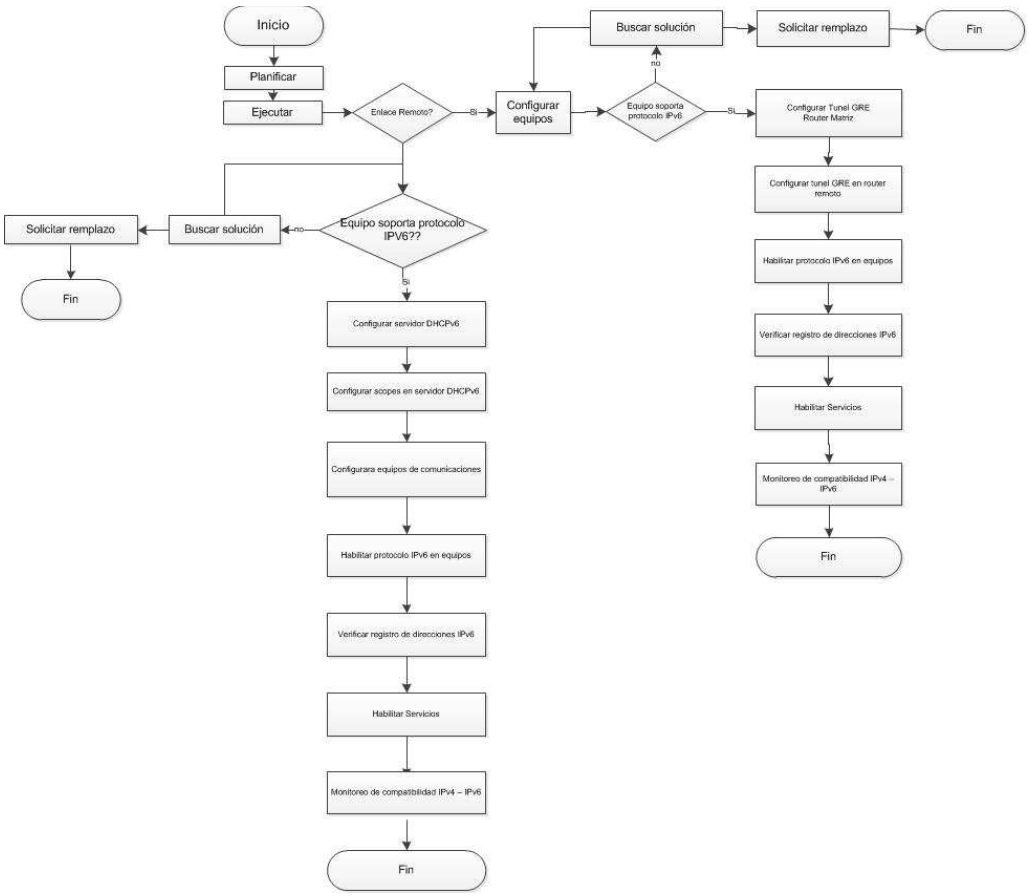


Figura 42. Estrategia de migración técnica

Para realizar la configuración el proceso de migración de la red interna se deberá tomar en cuenta lo siguientes:

- Se realizará la planificación del trabajo en base a un cronograma que se muestra se muestra posteriormente en la tabla 10.
- Se procederá a ejecutar el proceso de migración.
- Se ejecutará la configuración de los equipos.

- Se evaluará a los equipos que formarán parte del proceso de migración, véase tabla 11.
- Si los equipos soportan el protocolo IPv6 continuará las tareas de migración.
- En caso que el equipo no soporte el protocolo IPv6 se procederá a buscar alternativas para que este pueda integrarse a las tareas de migración.
- Como alternativas se podrá realizar actualizaciones de software o firmware.
- Si de ser el caso el equipo no llega a soporta al protocolo IPv6 se procederá con la solicitud de remplazo del mismo.
- Configurara el servidor DHCPv6.
- Configurar los equipos de comunicaciones estos son los switches tanto de core como de acceso.
- Posteriormente se habilitará el protocolo IPv6 en los equipos clientes.
- Una vez que se verifica que el protocolo haya sido habilitado se procederá verificar el registro de la dirección IPv6.
- Luego que constatamos la asignación correcta de la dirección se procederá a habilitar los servicios.
- Una vez pasadas estas etapas se constatará la compatibilidad y buen funcionamiento de los protocolos IPv4 e IPv6.

Cuando se trate de configurar las sucursales para que se integren al proceso de migración al protocolo IPv6 se procederá con las siguientes tareas.

- Se realizará la planificación del trabajo en base a un cronograma que se muestra se muestra posteriormente en la tabla 10.
- Se procederá a ejecutar el proceso de migración.
- Se ejecutará la configuración de los equipos.
- Se evaluará a los equipos que formarán parte del proceso de migración, véase tabla 11.
- Si los equipos soportan el protocolo IPv6 continuará las tareas de migración.

- En caso que el equipo no soporte el protocolo IPv6 se procederá a buscar alternativas para que este pueda integrarse a las tareas de migración.
- Como alternativas se podrá realizar actualizaciones de software o firmware.
- Si de ser el caso el equipo no llega a soporta al protocolo IPv6 se procederá con la solicitud de remplazo del mismo.
- Como tarea inicial será configurar túneles GRE en el enrutador matriz.
- Configurar túnel GRE en enrutador de la sucursal.
- Habilitar el protocolo IPv6 en la interface LAN del enrutador de la sucursal.
- Posteriormente se habilitará el protocolo IPv6 en los equipos clientes.
- Una vez que se verifica que el protocolo haya sido habilitado se procederá verificar el registro de la dirección IPv6.
- Luego que constatamos la asignación correcta de la dirección se procederá a habilitar los servicios.
- Una vez pasadas estas etapas se constatará la compatibilidad y buen funcionamiento de los protocolos IPv4 e IPv6.

4. Pruebas de la solución y análisis económico

4.1. Introducción

En el presente trabajo se han evaluado las diferentes técnicas que existen para una migración de un protocolo IPv4 a un protocolo IPv6, en este capítulo se mostrará los resultados obtenidos tras realizar las simulaciones del caso, adicionalmente se realizará un análisis económico en lo referente a los costos para ejecutar el proyecto.

4.2 DHCP

Para la asignación de direcciones IP la Secretaría de Hidrocarburos utiliza un servidor con sistema operativo Windows 2008 server en el cual tiene configurado el servicio de DHCP para la asignación de direcciones IPv4, se toma el mismo modelo de asignación de direcciones y se crea los ámbitos necesarios para asignación de direcciones IPv6 en las vlans configuradas.

Una forma de configurar del servicio DHCPv6 es sin estado, al momento de habilitar esta opción la asignación de direcciones IPv6 la realiza de forma automática el equipo terminal y lo único que entrega el servidor es información adicional como DNS y puerta de enlace.

Al deshabilitar la opción sin estado la asignación de direcciones IPv6 lo realiza el servidor DHCPv6, en este caso el servidor entrega toda la información al cliente es decir la dirección IPv6, DNS, puerta de enlace, entre otros.

En el presente trabajo de titulación la asignación de direcciones para los equipos a realizar las pruebas de laboratorio se lo asignarán de forma estática debido a que en el software simulación Packet Tracert no tiene disponible un servidor DHCPv6.

En la figura 43, se verifica como iniciar la instalación del servicio DHCP en un ambiente Windows 2008 Server, para lo cual lo primero que vamos a realizar es agregar la función DHCP.

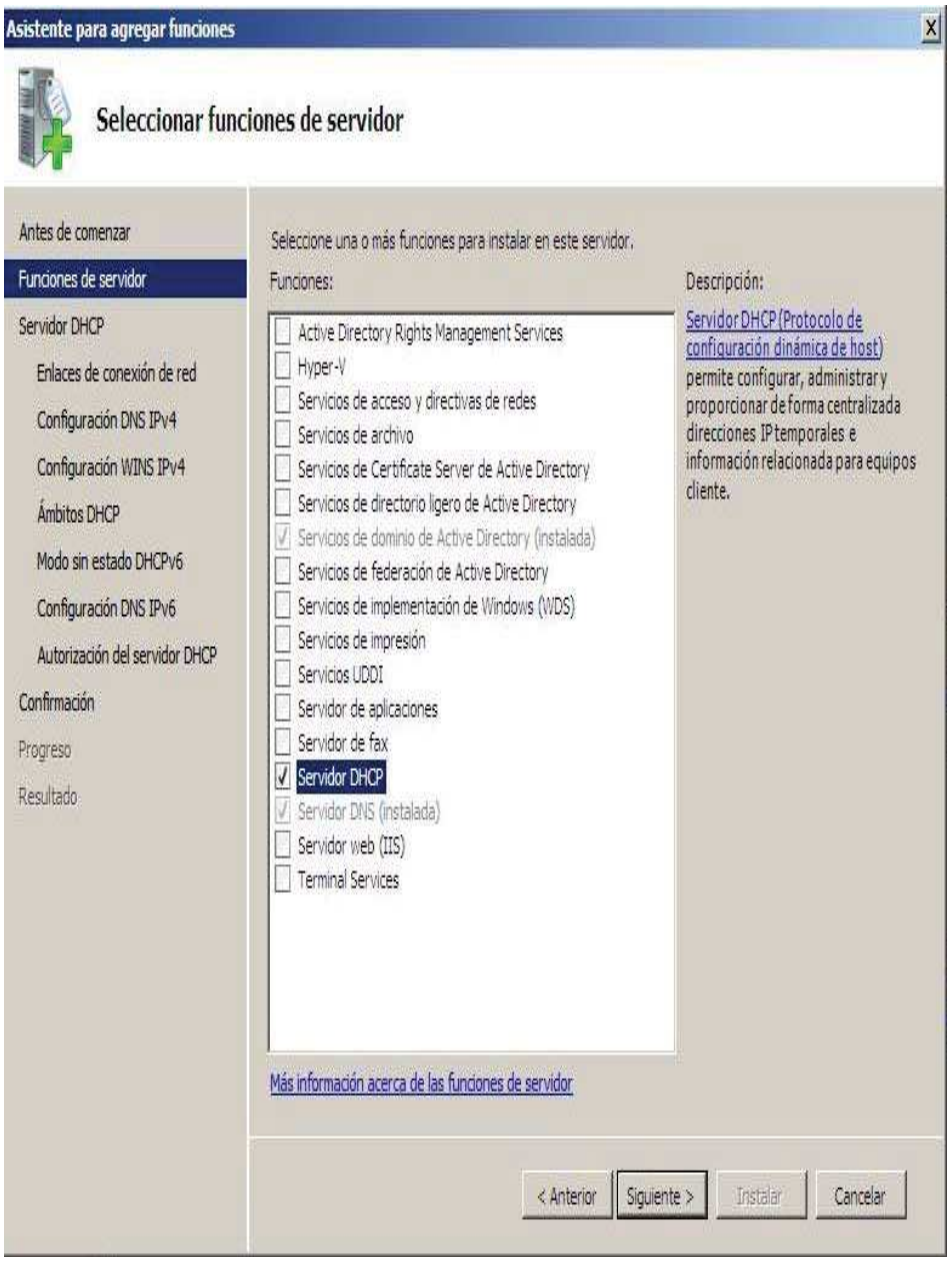


*Figura 43.*Agregar servicio DHCP en servidor Windows 2008 server

En la figura 44, se verifica la configuración del modo sin estado, que se utiliza en la instalación del servicio de DHCPv6 del sistema operativo Microsoft Windows 2008 server.

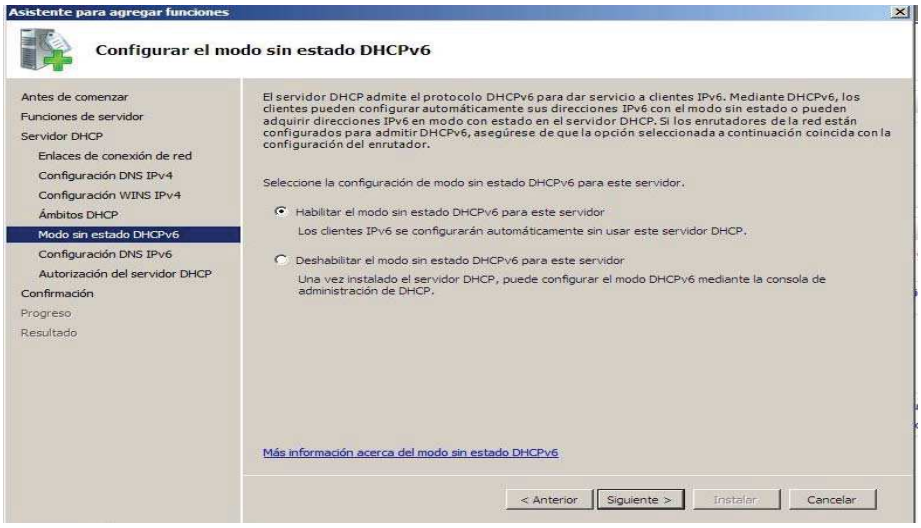


Figura 44. Configuración de servidor DHCPv6 modo sin estado

En la figura 45, se muestra el resumen de la configuración del servidor DHCP.

Figura 45. Resumen de la configuración de servidor DHCPv6

En la figura 46, Se muestra la configuración de una tarjeta de red de un PC que utilizará los protocolos IPv4 e IPv6.

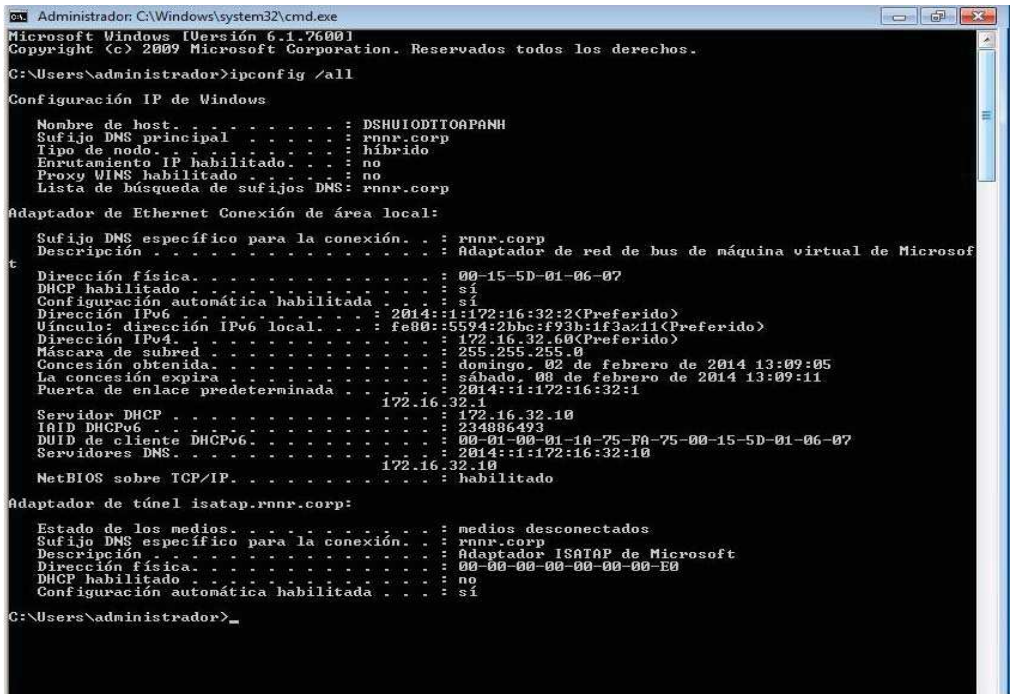


Figura 46. Configuración de una interface de red de un equipo

En la figura 47, se muestra una prueba de conectividad desde un cliente windows hacia el servidor mediante el protocolo IPv6.

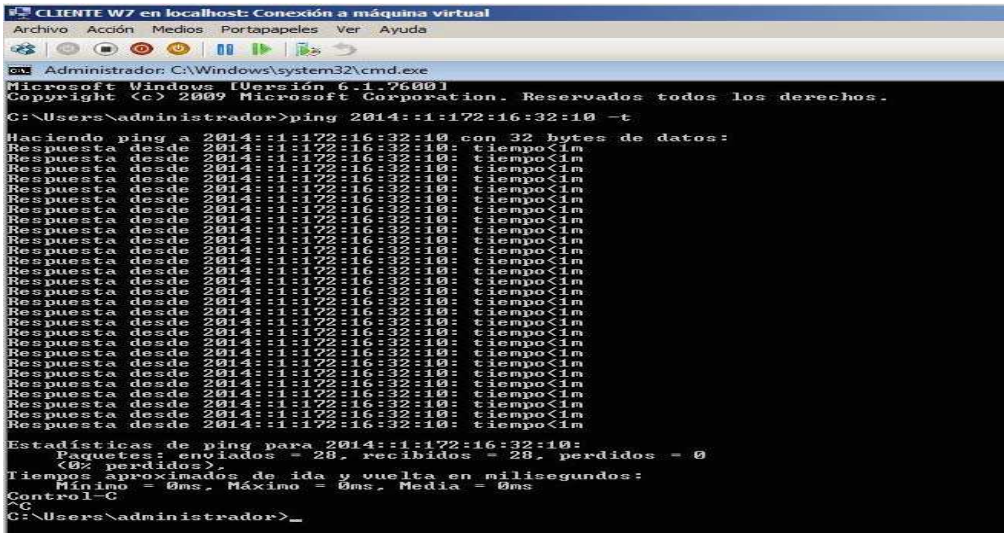


Figura 47. Prueba de conectividad con el protocolo IPv6

En la figura 48, se prueba el acceso a un servicio web IPv6 desde un equipo con figurado con IPv4/IPv6.

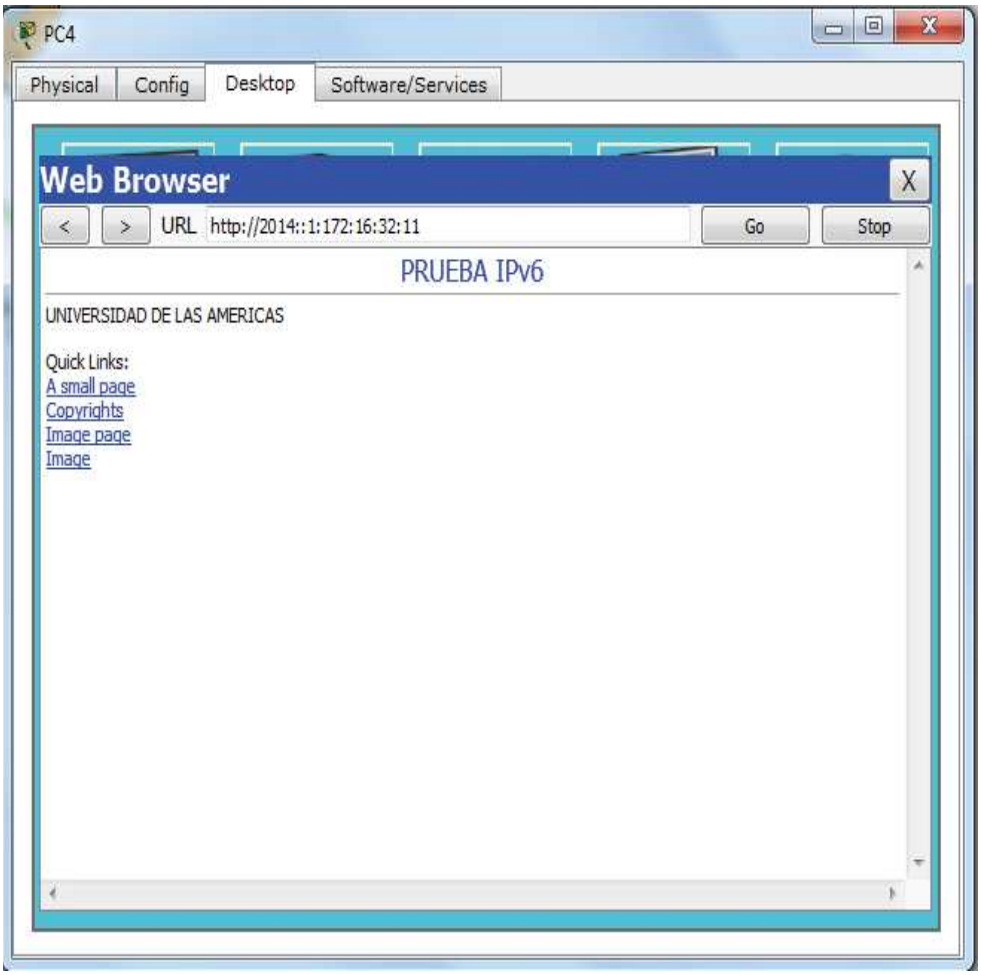


Figura 48. Prueba de un servicio IPv6

4.3 Configuración de equipos de comunicaciones

En lo referente a la conectividad de la red vamos a realizar la simulación de la propuesta de migración hacia un nuevo protocolo de comunicaciones IPv6 en un software de la empresa Cisco, este programa se llama Packet Tracert Versión 6.0.1.0011.

Tomando en cuenta que la convivencia de los protocolos en estudio será la mejor opción, esta técnica se la conoce como Dual Stack o doble pila.

En la figura 49, se muestra el diagrama de red que utiliza la Secretaría de Hidrocarburos y que será configurado para soportar los protocolos IPv4 e IPv6.

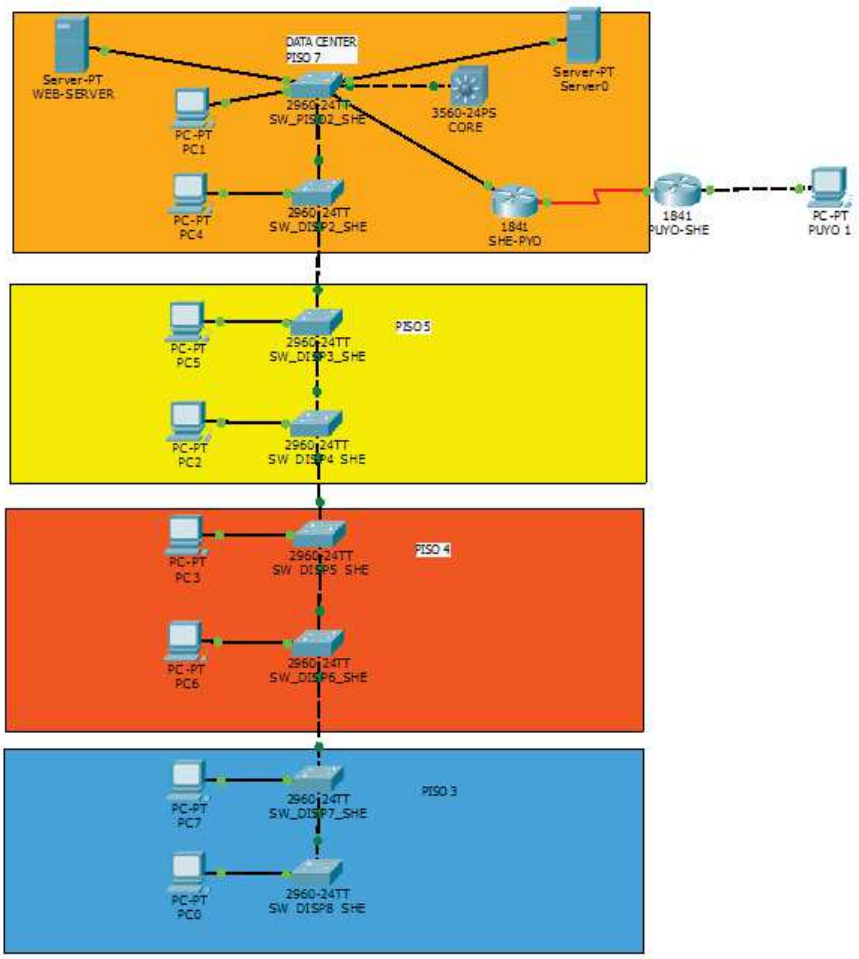


Figura 49. Diagrama de red a configurar y realizar el laboratorio

En la figura 50, se verifica la configuración de switch de core, en este equipo se habilito IPv6 en las vlan 2, 3 y 11.

```
CORE_SHE#sh run
hostname CORE_SHE
!
ip routing
!
ipv6 unicast-routing
!
interface GigabitEthernet0/1
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/2
 spanning-tree vlan 2 port-priority 144
!
interface Vlan1
 no ip address
 shutdown
!
interface Vlan2
ip address 172.16.32.1 255.255.255.0
ip helper-address 172.16.32.10
 ipv6 address 2014::1:172:16:32:1/64
!
interface Vlan3
ip address 172.16.110.1 255.255.255.0
ip helper-address 172.16.32.10
 ipv6 address 2014::2:172:16:110:1/64
!
interface Vlan6
ip address 172.16.115.1 255.255.255.0
!
interface Vlan11
ip address 172.16.118.1 255.255.255.0
 ipv6 address 2014::9:172:16:118:1/64
 ipv6 rip uiopyo enable
!
ipv6 router rip uiopyo
!
End
```

Figura 50. Archivo de configuración en switch de core

El diseño de la red basada en el protocolo IPv4 fue realizada previamente por la entidad, en la figura 51, se muestra como configurar dentro de una interface vlan tanto la direcciónIPv4 como la dirección IPv6.

```
CORE_SHE(config)#interface vlan 5
CORE_SHE(config-if)#ip address 172.16.114.1 255.255.255.0
CORE_SHE(config-if)#ipv6 address 2014::4:172:16:114:1/64
```

Figura 51. Configuración de IPv4 e IPv6 en switch de core

El direccionamiento ingresado en estas interfaces a nivel de red pasa a ser la puerta de enlace de estas subredes.

4.4 Enrutamiento intervlan IPv6

En el switch de core se debe habilitar el enrutamiento intervlan para que las subredes IPv6 se puedan ver entre sí, en la figura 52 se muestra como agregar este comando.

```
CORE_SHE(config)#ipv6 unicast-routing
```

Figura 52. Comando para habilitar el enrutamiento intervlan IPv6

4.5 Enlaces remotos

La Secretaría de Hidrocarburos mantiene al momento una sucursal en la ciudad de El Puyo conectada a través de un enlace de datos con su matriz ubicada en la ciudad de Quito, sus equipos trabajan con el protocolo IPv4, en el software emulador Packet Tracert se realiza la migración al protocolo IPv6 en un equipo de la red remota, utilizando un túnel GRE para la encapsulación y transporte de los paquetes IPv6, en la figura 53 se mostrará las configuraciones realizadas.

```
Secretaria#
!
hostname Secretaria
!
ipv6 unicast-routing
!
spanning-tree mode pvst
!
interface Tunnel0
 no ip address
mtu 1476
 ipv6 address 2014::11:10:10:10:2/64
 tunnel source Serial0/0/0
 tunnel destination 10.10.10.2
 tunnel mode ipv6ip
!
interface FastEthernet0/0
ip address 172.16.118.2 255.255.255.0
 duplex auto
 speed 100
 ipv6 address 2014::9:172:16:118:2/64
!
interface Serial0/0/0
ip address 10.10.10.1 255.255.255.252
clock rate 64000
!
ipv6 route ::/0 2014::11:10:10:10:1
!
End
```

Figura 53. Archivo de configuración del enrutador de enlace de datos

Hay que considerar que manejamos direcciones tanto IPv4 como IPv6 en la interface FastEthernet0/0, esta nos permite la conectividad con la red interna, la dirección IP del túnel es IPv6, el origen es la interface donde se realiza la conexión con la sucursal y su destino es la dirección IPv4 del equipo destino.

En la figura 54, se verificará la configuración que se realizará en el enrutador que se encuentra en la sucursal El Puyo.

```
SHE_PUYO#
!
hostname SHE_PUYO
!
ipv6 unicast-routing
!
interface Tunnel0
 no ip address
mtu 1476
 ipv6 address 2014::11:10:10:10:1/64
 tunnel source Serial0/0/0
 tunnel destination 10.10.10.1
 tunnel mode ipv6ip
!
interface FastEthernet0/0
 no ip address
 duplex auto
 speed 100
 ipv6 address 2014::10:172:16:33:254/64
!
interface Serial0/0/0
ip address 10.10.10.2 255.255.255.0
!
ip classless
ip route 0.0.0.0 0.0.0.0 Serial0/0/0
!
ipv6 route ::/0 2014::11:10:10:10:2
!
End
```

*Figura 54.*Archivo de configuración de enrutador remoto

En este equipo se realiza una configuración parecida al enrutador ubicado en la matriz con la diferencia que el direccionamiento de la interface FastEthernet0/0 que conecta la red LAN de la sucursal, seráúnicamente con el protocolo IPv6.

Una vez revisado las diferentes configuraciones de la red de datos y analizado los cambios que se deberán realizar en los equipos para la convivencia del

protocolo IPv6 e IPv4, ahora se tendrá que revisar cuáles serán los costos económicos que tendremos al ejecutar el proyecto de migración.

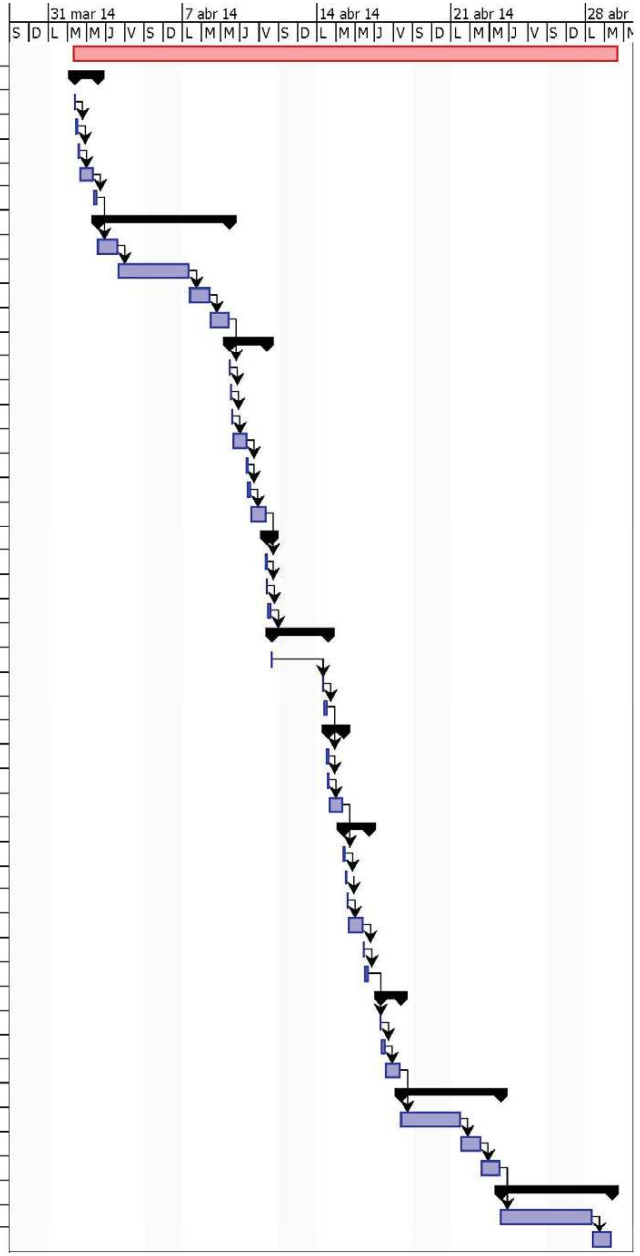
4.6 Cronograma de trabajo

Con el fin de cumplir con las tareas de migración, en la tabla 10 se muestra el cronograma de trabajo, en el mismo constan los acciones a realizar en los diferentes equipos el tiempo a ejecutarlo y la fecha de culminación de mencionado trabajo.

En donde se resaltan las tareas a realizar en cada uno de los procesos de migración.

Tabla 10. Cronograma de trabajo

	Nombre	Duración	Inicio	Terminado	Predecesores	Nombres del Recurso
1	Cronograma de trabajo migración IPv4/IPv6	21 days?	01/04/14 08:00 AM	29/04/14 05:00 PM		
2	**Servidores**	**1,5 days**	**01/04/14 09:00 AM**	**02/04/14 02:00 PM**		
3	Agregar el servicio de DHCPv6	0,25 days	01/04/14 09:00 AM	01/04/14 11:00 AM		
4	Configurar Ambito	0,25 days	01/04/14 11:00 AM	01/04/14 02:00 PM	3	
5	Configurar DNS	0,25 days	01/04/14 02:00 PM	01/04/14 04:00 PM	4	
6	Configurar registros PTR	0,25 days	01/04/14 04:00 PM	02/04/14 09:00 AM	5	
7	Pruebas de funcionamiento	0,5 days	02/04/14 09:00 AM	02/04/14 02:00 PM	6	
8	**Equipos Clientes (146 EQUIPOS)**	**4,75 days?**	**02/04/14 02:00 PM**	**09/04/14 11:00 AM**		
9	Verificar protocolo de Internet versión 6 (TCP/IPv6)	1,25 days?	02/04/14 02:00 PM	03/04/14 04:00 PM	7	
10	Verificar configuración automática de protocolo	1,25 days?	03/04/14 04:00 PM	07/04/14 09:00 AM	9	
11	Verificar dirección IP con comando IPCONFIG	1,25 days?	07/04/14 09:00 AM	08/04/14 11:00 AM	10	
12	Pruebas de funcionamiento	1 day?	08/04/14 11:00 AM	09/04/14 11:00 AM	11	
13	**EQUIPO SWITCH DE CORE CISCO 3560**	**1,75 days?**	**09/04/14 11:00 AM**	**11/04/14 09:00 AM**		
14	Verificar versión de IOS	0,125 days?	09/04/14 11:00 AM	09/04/14 01:00 PM	12	
15	IOS CISCO	0,125 days?	09/04/14 01:00 PM	09/04/14 02:00 PM	14	
16	Realizar respaldo de configuración	0,25 days?	09/04/14 02:00 PM	09/04/14 04:00 PM	15	
17	Actualizar IOS	0,25 days?	09/04/14 04:00 PM	10/04/14 09:00 AM	16	
18	Verificar IOS	0,125 days?	10/04/14 09:00 AM	10/04/14 10:00 AM	17	
19	Configurar IPv6 en VLANs existentes	0,375 days?	10/04/14 10:00 AM	10/04/14 02:00 PM	18	
20	Pruebas de funcionamiento	0,5 days?	10/04/14 02:00 PM	11/04/14 09:00 AM	19	
21	**EQUIPOS SWITCH DE ACCESO CISCO 2960 (8 EQUIPOS)**	**0,75 days?**	**11/04/14 09:00 AM**	**11/04/14 04:00 PM**		
22	Verificar versión de IOS	0,125 days?	11/04/14 09:00 AM	11/04/14 10:00 AM	20	
23	Configurar IPv6 de administración	0,125 days?	11/04/14 10:00 AM	11/04/14 11:00 AM	22	
24	Pruebas de funcionamiento	0,5 days?	11/04/14 11:00 AM	11/04/14 04:00 PM	23	
25	**CENTRAL TELEFÓNICA**	**0,75 days?**	**11/04/14 04:00 PM**	**14/04/14 02:00 PM**	**24**	
26	Verificar versión de IOS	0,125 days?	11/04/14 04:00 PM	11/04/14 05:00 PM		
27	Configurar IPv6 en interface	0,125 days?	14/04/14 08:00 AM	14/04/14 09:00 AM	26	
28	Pruebas de funcionamiento	0,5 days?	14/04/14 09:00 AM	14/04/14 02:00 PM	27	
29	**ACS**	**0,5 days?**	**14/04/14 02:00 PM**	**15/04/14 09:00 AM**		
30	Verificar versión de IOS	0,125 days?	14/04/14 02:00 PM	14/04/14 03:00 PM	28	
31	Configurar IPv6 en interface	0,125 days?	14/04/14 03:00 PM	14/04/14 04:00 PM	30	
32	Pruebas de funcionamiento	0,25 days?	14/04/14 04:00 PM	15/04/14 09:00 AM	31	
33	**ACCESS POINT CISCO AIRONET 1260 (3 EQUIPOS)**	**1,875 days?**	**15/04/14 09:00 AM**	**16/04/14 05:00 PM**		
34	Verificar versión de IOS	0,375 days?	15/04/14 09:00 AM	15/04/14 01:00 PM	32	
35	IOS AIRONET CISCO	0,125 days?	15/04/14 01:00 PM	15/04/14 02:00 PM	34	
36	Realizar respaldo de configuración	0,25 days?	15/04/14 02:00 PM	15/04/14 04:00 PM	35	
37	Actualizar IOS	0,5 days?	15/04/14 04:00 PM	16/04/14 11:00 AM	36	
38	Verificar IOS	0,125 days?	16/04/14 11:00 AM	16/04/14 01:00 PM	37	
39	Pruebas de funcionamiento	0,5 days?	16/04/14 01:00 PM	16/04/14 05:00 PM	38	
40	**CISCO ASA 5520 (2 EQUIPOS)**	**1,25 days?**	**17/04/14 08:00 AM**	**18/04/14 10:00 AM**		
41	Verificar versión de IOS	0,25 days?	17/04/14 08:00 AM	17/04/14 10:00 AM	39	
42	Configurar IPv6 en interface	0,5 days?	17/04/14 10:00 AM	17/04/14 03:00 PM	41	
43	Pruebas de funcionamiento	0,5 days?	17/04/14 03:00 PM	18/04/14 10:00 AM	42	
44	**TELEFONOS CISCO IP PHONE 7911 (90 EQUIPOS)**	**3,5 days?**	**18/04/14 10:00 AM**	**23/04/14 03:00 PM**		
45	Verificar versión de IOS	1,25 days?	18/04/14 10:00 AM	21/04/14 01:00 PM	43	
46	Configurar IPv6 en interface	1,25 days?	21/04/14 01:00 PM	22/04/14 03:00 PM	45	
47	Pruebas de funcionamiento	1 day?	22/04/14 03:00 PM	23/04/14 03:00 PM	46	
48	**CAPACITACION**	**3,5 days?**	**23/04/14 03:00 PM**	**29/04/14 10:00 AM**		
49	Capación personal técnico (3 personas)	2,5 days?	23/04/14 03:00 PM	28/04/14 10:00 AM	47	
50	Capacitación usuario final	1 day?	28/04/14 10:00 AM	29/04/14 10:00 AM	49	



4.7 Análisis económico

Para ejecutar el proceso de migración de un protocolo IPv4 a un protocolo IPv6 es necesario realizar varios trabajos en los equipos informáticos que pertenecen a la entidad los mismos que ocasionarán un gasto económico, razón por la que se ha realizado una evaluación de costos de las tareas a realizar.

En la tabla 11 se realiza la evaluación de los equipos tecnológicos que estarán en el proceso de migración.

Tabla 11.Evaluación de equipos de telecomunicaciones

ITEM	DETALLE	CANTIDAD	SOPORTA IPv6
1	Catalyst 3560E 12 Ten GE (X2) ports, IPS software	1	NO
2	Catalyst 2960S 24 GigE PoE 370W, 4 x SFP LAN Base	8	SI
3	802.11a/g/n Standalone AP; Ext Ant; A Reg Domain	3	NO
4	ASA 5520 Appliance with SW, HA, 4GE+1FE, DES	2	SI
5	3945 Voice Bundle w/ PVDM3-64,FL-CME-SRST-25, UC License PAK	1	SI
6	ACS 1121 Appliance With 5.x SW And Base license	1	SI
7	Cisco UC Phone 9971, Charcoal, SlmHndst with Camera	3	SI
8	Cisco Unified IP Phone 7965, Gig Ethernet, Color	1	SI
9	7916 IP Phone Color Expansion Module	1	SI
10	7911 G IP Phone	60	SI
11	Cisco Unity Express Network Module Enhanced (8 ports Incl)	1	SI
12	Astaro ASG320	1	SI

En la tabla 12, se muestra los costos de las tareas a realizar en cada uno de los equipos, en el proyecto formarán parte de la implementación profesionales con escalas salariales SP7 y SP5, adicionalmente se toma en cuenta los equipos a utilizar y se detalla sus costos de acuerdo a las horas por tarea a realizar.

Tabla 12. Detalle de costos de los trabajos a realizar

Técnico a realizar	Cantidad de técnicos	Sueldo del técnico	Detalle	Horas hombre	Costo unitario	Costo Parcial	Equipos	Costo unitario	Costo Parcial	Costo de implementación
Ingeniero SP7	1	1676	**Servidores**							$ 325,70
			Agregar el servicio de DHCPv6	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Configurar Ambito	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Configurar DNS	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Configurar registros PTR	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	4	$ 10,48	$ 41,90	1	$ 40,00	$ 40,00	
Ingeniero SP5	2	1212	**Equipos Clientes (146 EQUIPOS)**							$ 735,70
			Verificar protocolo de Internet versión 6 (TCP/IPv6)	10	$ 15,15	$ 151,50	1	$ 40,00	$ 40,00	
			Verificar configuración automática de protocolo	10	$ 15,15	$ 151,50	1	$ 40,00	$ 40,00	
			Verificar dirección IP con comando IPCONFIG	10	$ 15,15	$ 151,50	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	8	$ 15,15	$ 121,20	1	$ 40,00	$ 40,00	
Ingeniero SP7	1	1676	**EQUIPO SWITCH DE CORE CISCO 3560**							$ 2.776,18
			Verificar versión de IOS	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
			IOS CISCO	1	$ 0,00	$ 0,00	1	$ 2.400,00	$ 2.400,00	
			Realizar respaldo de configuración	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Actualizar IOS	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Verificar IOS	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
			Configurar IPv6 en VLANs existentes	3	$ 10,48	$ 31,43	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	4	$ 10,48	$ 41,90	1	$ 40,00	$ 40,00	
Ingeniero SP7	1	1676	**EQUIPOS SWITCH DE ACCESO CISCO 2960 (8 EQUIPOS)**							$ 182,85
			Verificar versión de IOS	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
			Configurar IPv6 de administración	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	4	$ 10,48	$ 41,90	1	$ 40,00	$ 40,00	
Ingeniero SP7	1	1676	**CENTRAL TELEFÓNICA**							$ 182,85
			Verificar versión de IOS	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
			Configurar IPv6 en interface	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	4	$ 10,48	$ 41,90	1	$ 40,00	$ 40,00	
Ingeniero SP7	1	1676	**ACS**							$ 151,43
			Verificar versión de IOS	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
			Configurar IPv6 en interface	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
Ingeniero SP7	1	1676	**ACCESS POINT CISCO AIRONET 1260 (3 EQUIPOS)**							$ 1.146,65
			Verificar versión de IOS	3	$ 10,48	$ 31,43	1	$ 40,00	$ 40,00	
			IOS AIRONET CISCO	1	$ 0,00	$ 0,00	1	$ 800,00	$ 800,00	
			Realizar respaldo de configuración	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Actualizar IOS	4	$ 10,48	$ 41,90	1	$ 40,00	$ 40,00	
			Verificar IOS	1	$ 10,48	$ 10,48	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	4	$ 10,48	$ 41,90	1	$ 40,00	$ 40,00	
Ingeniero SP7	1	1676	**CISCO ASA 5520 (3 EQUIPOS)**							$ 203,80
			Verificar versión de IOS	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Configurar IPv6 en interface	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	4	$ 10,48	$ 41,90	1	$ 40,00	$ 40,00	
Ingeniero SP5	2	1212	**TELEFONOS CISCO IP PHONE 7911 (90 EQUIPOS)**							$ 544,20
			Verificar versión de IOS	10	$ 15,15	$ 151,50	1	$ 40,00	$ 40,00	
			Configurar IPv6 en interface	10	$ 15,15	$ 151,50	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	8	$ 15,15	$ 121,20	1	$ 40,00	$ 40,00	
Ingeniero SP7	1	1676	**ENLACES REMOTOS**							$ 224,75
			Verificar versión de IOS	2	$ 10,48	$ 20,95	1	$ 40,00	$ 40,00	
			Configurar túneles	4	$ 10,48	$ 41,90	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	4	$ 10,48	$ 41,90	1	$ 40,00	$ 40,00	
Ingeniero SP5	1	1212	**CONFIGURACION EQUIPOS SUCURSAL**							$ 281,20
			Verificar protocolo de Internet versión 6 (TCP/IPv6)	2	$ 15,15	$ 30,30	1	$ 40,00	$ 40,00	
			Verificar configuración automática de protocolo	4	$ 15,15	$ 60,60	1	$ 40,00	$ 40,00	
			Verificar dirección IP con comando IPCONFIG	2	$ 15,15	$ 30,30	1	$ 40,00	$ 40,00	
			Pruebas de funcionamiento	4	$ 15,15	$ 60,60	1	$ 40,00	$ 40,00	
Ingeniero SP7	1	1676	**CAPACITACION**							$ 394,25
			Capación personal técnico (3 personas)	20	$ 10,48	$ 209,50	1	$ 40,00	$ 40,00	
			Capacitación usuario final	10	$ 10,48	$ 104,75	1	$ 40,00	$ 40,00	
									Costo Parcial	$ 7.149,55
									Imprevistos	$ 1.429,91

En la tabla 13, se realiza un cuadro comparativo en relación a que el trabajo lo puede realizar personal propio de la entidad con una empresa contratada considerada como tercero, realizando esta relación se observa que al ejecutar el proceso de migración por parte de personal propio de la entidad resulta beneficioso obteniendo un 34,80 % de ahorro.

Tabla 13. Análisis comparativo entre trabajo a realizar con técnicos de la entidad y empresa contratada

Detalle	Horas hombre	Costo unitario	Costo Parcial	Valor de implementación	Costo de Implementación	UTILIDAD	% UTILIDAD
Servidores				$ 720,00	$ 325,70	$ 394,30	54,76%
Agregar el servicio de DHCPv6	2	$ 60,00	$ 120,00				
Configurar Ambito	2	$ 60,00	$ 120,00				
Configurar DNS	2	$ 60,00	$ 120,00				
Configurar registros PTR	2	$ 60,00	$ 120,00				
Pruebas de funcionamiento	4	$ 60,00	$ 240,00				
Equipos Clientes (146 EQUIPOS)				$ 1.520,00	$ 735,70	$ 784,30	51,60%
Verificar protocolo de Internet versión 6 (TCP/IPv6)	10	$ 40,00	$ 400,00				
Verificar configuración automática de protocolo	10	$ 40,00	$ 400,00				
Verificar dirección IP con comando IPCONFIG	10	$ 40,00	$ 400,00				
Pruebas de funcionamiento	8	$ 40,00	$ 320,00				
EQUIPO SWITCH DE CORE CISCO 3560				$ 2.920,00	$ 2.776,18	$ 143,83	4,93%
Verificar versión de IOS	1	$ 40,00	$ 40,00				
IOS CISCO	1	$ 2.400,00	$ 2.400,00				
Realizar respaldo de configuración	2	$ 40,00	$ 80,00				
Actualizar IOS	2	$ 40,00	$ 80,00				
Verificar IOS	1	$ 40,00	$ 40,00				
Configurar IPv6 en VLANs existentes	3	$ 40,00	$ 120,00				
Pruebas de funcionamiento	4	$ 40,00	$ 160,00				
EQUIPOS SWITCH DE ACCESO CISCO 2960 (8 EQUIPOS)				$ 240,00	$ 182,85	$ 57,15	23,81%
Verificar versión de IOS	1	$ 40,00	$ 40,00				
Configurar IPv6 de administración	1	$ 40,00	$ 40,00				
Pruebas de funcionamiento	4	$ 40,00	$ 160,00				
CENTRAL TELEFÓNICA				$ 240,00	$ 182,85	$ 57,15	23,81%
Verificar versión de IOS	1	$ 40,00	$ 40,00				
Configurar IPv6 en interface	1	$ 40,00	$ 40,00				
Pruebas de funcionamiento	4	$ 40,00	$ 160,00				
ACS				$ 160,00	$ 151,43	$ 8,57	5,36%
Verificar versión de IOS	1	$ 40,00	$ 40,00				
Configurar IPv6 en interface	1	$ 40,00	$ 40,00				
Pruebas de funcionamiento	2	$ 40,00	$ 80,00				
ACCESS POINT CISCO AIRONET 1260 (3 EQUIPOS)				$ 1.360,00	$ 1.146,65	$ 213,35	15,69%
Verificar versión de IOS	3	$ 40,00	$ 120,00				
IOS AIRONET CISCO	1	$ 800,00	$ 800,00				
Realizar respaldo de configuración	2	$ 40,00	$ 80,00				
Actualizar IOS	4	$ 40,00	$ 160,00				
Verificar IOS	1	$ 40,00	$ 40,00				
Pruebas de funcionamiento	4	$ 40,00	$ 160,00				
CISCO ASA 5520 (3 EQUIPOS)				$ 320,00	$ 203,80	$ 116,20	36,31%
Verificar versión de IOS	2	$ 40,00	$ 80,00				
Configurar IPv6 en interface	2	$ 40,00	$ 80,00				
Pruebas de funcionamiento	4	$ 40,00	$ 160,00				
TELEFONOS CISCO IP PHONE 7911 (90 EQUIPOS)				$ 1.120,00	$ 544,20	$ 575,80	51,41%
Verificar versión de IOS	10	$ 40,00	$ 400,00				
Configurar IPv6 en interface	10	$ 40,00	$ 400,00				
Pruebas de funcionamiento	8	$ 40,00	$ 320,00				
ENLACES REMOTOS				$ 400,00	$ 224,75	$ 175,25	43,81%
Verificar versión de IOS	2	$ 40,00	$ 80,00				
Configurar túneles	4	$ 40,00	$ 160,00				
Pruebas de funcionamiento	4	$ 40,00	$ 160,00				
CONFIGURACION EQUIPOS SUCURSAL				$ 480,00	$ 281,20	$ 198,80	41,42%
Verificar protocolo de Internet versión 6 (TCP/IPv6)	2	$ 40,00	$ 80,00				
Verificar configuración automática de protocolo	4	$ 40,00	$ 160,00				
Verificar dirección IP con comando IPCONFIG	2	$ 40,00	$ 80,00				
Pruebas de funcionamiento	4	$ 40,00	$ 160,00				
CAPACITACION				$ 1.200,00	$ 394,25	$ 805,75	67,15%
Capación personal técnico (3 personas)	20	$ 40,00	$ 800,00				
Capacitación usuario final	10	$ 40,00	$ 400,00				

		TERCERO	SHE		
Costo Parcial	Costo Parcial	$ 9.800,00	$ 7.149,55	$ 3.530,45	36,03%
Imprevistos	Imprevistos	$ 1.960,00	$ 1.429,91	$ 706,09	36,03%
Costo total	**Costo total**	**$ 11.760,00**	**$ 8.579,46**	**$ 4.236,54**	**36,03%**

En la figura 55, se muestra una gráfica donde se demuestra lo indicado realizando el análisis comparativo de implementación.

Figura 55. Análisis comparativo de implementación entre personal propio y empresa contratada.

En la tabla 14 se muestra un resumen general de costos que tendrá la implementación del proyecto de migración técnica, se considera un 20 % del costo parcial para posibles eventualidades que se presenten durante los trabajos propuestos.

Tabla 14.Resumen general de costos

	TERCERO	SHE		
Costo Parcial	$ 9.800,00	$ 7.109,55	$ 3.570,45	36,43%
Imprevistos	$ 1.960,00	$ 1.421,91	$ 714,09	36,43%
Costo total	**$ 11.760,00**	**$ 8.531,46**	**$ 4.284,54**	**36,43%**

5. Conclusiones y Recomendaciones

5.1 Conclusiones

- La infraestructura tecnológica que posee la entidad se basa en una modelo jerárquico donde sobresalen un equipo switch core y ocho switches de acceso, esta estructura nos ayuda a segmentar el tráfico y tener varias subredes con direccionamiento diferente.

- Los parámetros utilizados en la red LAN se basan en direcciones de tipo privado, estas a su vez están asignadas mediante VLAN a los diferentes segmentos de red.

- Los parámetros utilizados en la red WAN se establecen de acuerdo al direccionamiento e infraestructura asignada por el proveedor de servicios de datos e Internet CNT.

- Al ser IPv6 un sistema de direccionamiento de 128 bits, nos permite tener un número de direcciones IP, que sirve para la conectividad de millones de dispositivos dentro de una misma red, se utiliza subredes IPv6 con el prefijo /64 para cada una de las VLANS que posee la entidad.

- Los equipos que posee la entidad tienen todas las características para realizar planes de migración al protocolo IPv6, en mucho de los casos lo único que se deberá realizar son la actualizaciones de los sistemas de software base u IOS.

- Como mecanismo de migración se considera a mantener un doble direccionamiento tanto IPv4 como IPv6 como uno de los métodos más adecuados para realizar estudios o planes de migración, debido a que

los terminales podrán seguir utilizando las aplicaciones que trabajen tanto en IPv4 como en IPv6.

- Una de las características más relevantes del protocolo IPv6 es la seguridad que viene incluida dentro de este protocolo, además permite calidad de servicio, movilidad, etc.

- A nivel WAN el túnel IPV6 sobre IPv4 resulta lo más adecuado para el encaminamiento de paquetes IPv6 debido a que los proveedores de servicio de redes de datos aún no poseen sus redes configuradas con el protocolo IPv6.

- Se utilizó software de simulación de equipos de telecomunicaciones como el Packet Tracert 6.0.1 el mismo que nos permitió evidenciar el funcionamiento de la propuesta técnica planteada, para la parte de sistemas operativos se utilizó a Windows 2008 server para verificar el funcionamiento del servicio de DHCPv6.

- Al realizar el análisis económico se planteó una evaluación de costos utilizando a personal de la entidad con personal contratado, teniendo como resultado que el trabajo al realizar con personal propio tendrá un resultado favorable para la entidad.

5.2 Recomendaciones

- Con el fin de poder implementar el protocolo IPv6 se debe considerar que las nuevas aplicaciones sean diseñadas para soportar el protocolo IPv6.

- Hay que pensar que para poder administrar de una forma adecuada este nuevo modelo de direccionamiento se debe capacitar a los ingenieros

que estarán a cargo de estas labores, tanto en la parte teórica como en la práctica.

- Se debe considerar remplazar al equipo switch de core Cisco 3560 debido a que resulta más beneficios invertir en un switch de mejores características y que soporte IPv6 en lugar de realizar la actualización del IOS.

- Se debe planificar la convivencia de los protocolos IPv4 e IPv6 mientras se migran las aplicaciones a IPv6.

- Para el mejor funcionamiento de una red de datos con servicios IPv6 se deberá tomar en cuenta que el proveedor de servicios de Internet provea ya este tipo de direccionamiento ya que nos permitirá tener conectividad hacia el Internet.

Referencias

Loshin Pete. (2004). Theory, protocol, and practice.Estados Unidos de América, San Francisco: Elsevier.

Cicileo, G., Gagliano, R., O'Flaherty, C., Olvera, C., Palet, J., Rocha, M., Vives, A., (2009). IPv6 para todos. Argentina, Buenos Aires: E-Book.

McFarland, S., Sambi, M., Sharma, N., Hooda, S.,(2011). IPv6 for Enterprise Networks. Estados Unidos de América, Indianapolis: Cisco Press.

Americas Headquarters.,(2009). Cisco IOS IPv6 Configuration Guide.Estados Unidos de América, San Jose: Cisco Press.

Karlsson, B., (2003). ImplementingIPv6. Estados Unidos de América, Indianapolis: Cisco Press.

Cisco System. (2013). Cisco Networking Academy. Estados Unidos de América, Indianapolis: Cisco Press.

Postel, J. (1981). Protocolo de Internet. Recuperado el 18 de Octubre de 2013 de http://www.ietf.org/rfc/rfc791.txt.

Rekhter, E. (1996). Asignación de direcciones ara Internet privadas. Recuperado el 26 de Septiembre de 2013 de http://www.rfc-es.org/rfc/rfc1918-es.txt.

Deering, S., Hinden, R., (1998). Especificación Protocolo de Internet, Versión 6 (IPv6). Recuperado el 29 de Septiembre de 2013 de http://www.rfc-es.org/rfc/rfc2460-es.txt.

Deering, S., Hinden, R., (2003). Internet Protocol Version 6 (IPv6) Addressing Architecture. Recuperado el 02 de Octubre de 2013 de https://tools.ietf.org/html/rfc3513.

Srisuresh, P., Egevang, K., (2001). Traductor de Dirección de Red IP Tradicional (NAT tradicional). Recuperado el 19 de Octubre de 2013 de http://www.rfc-es.org/rfc/rfc3022-es.txt.

Conta, A., Deering, S., (1998).Generic Packet Tunneling in IPv6 Specification. Recuperado el 06 de Diciembre de 2013 de http://tools.ietf.org/rfc/rfc2473.txt.

Nordmark, E., Gilligan, R., (2005). Basic Transition Mechanisms for IPv6 Hosts and Routers. Recuperado el 25 de Diciembre de 2013 de http://tools.ietf.org/html/rfc4213.

Chown, T., (2006).Use of VLANs for IPv4-IPv6 Coeistencia in Enterprise Networks. Recuperado el 03 de Enero de 2014 de http://tools.ietf.org/rfc/rfc4554.txt.

Hanks, S., Li, T., Farinacci, D., Traina, P., (1994). Generic Routing Encapsulation (GRE). Recuperado el 14 de Enero de 2014 de http://tools.ietf.org/html/rfc1701.

Templin, F., Gleeson, T., Thaler, D., (2008).Intra-Site Automatic Tunnel Addressing Protocol (ISATAP).Recuperado el 20 de Febrero de 2014 de http://tools.ietf.org/html/rfc5214.

Carpenter, F., Moore, K.(2008). Connection of IPv6 Domains via IPv4 Clouds. Recuperado el 03 de Marzo de 2014 de http://www.ietf.org/rfc/rfc3056.txt.

Perez, E. (2012). IPv6 - Capítulo 01 - Curso de implementación de IPv6 en servidores Linux. Recuperado el 18 de Enero de 2014 de http://www.youtube.com/watch?v=0aDuJ6Bg2L0.

Perez, E. (2012). IPv6 - Capítulo 01 - Curso de implementación de IPv6 en servidores Linux. Recuperado el 18 de Enero de 2014 de http://www.youtube.com/watch?v=0aDuJ6Bg2L0.