UNIVERSIDAD NACIONAL

“PEDRO RUIZ GALLO”

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

TESIS DE GRADO

PREVIA A LA OBTENCIÓN DEL TITULO DE INGENIERO ELECTRÓNICO

Tema:

Migración de IPv4 a IPv6 para mejorar la seguridad y velocidad de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

PARA OPTAR EL TITULO PROFESIONAL DE INGENIERO ELECTRONICO

ELABORADO POR:

Manayay Ramírez Cristian Saul

Olivera Samamé Robert Edinson

ASESOR:

Segura Altamirano Segundo Francisco

LAMBAYEQUE – PERÚ

2015

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

Tema:

"Migración de IPv4 a IPv6 para mejorar la seguridad y velocidad de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo"

TESIS DE GRADO

Sustentada por los siguientes tesistas, para obtener el Título de:
INGENIERO ELECTRÓNICO

Manayay Ramírez Cristian Saul

Olivera Samamé Robert Edinson

Segura Altamirano Segundo Francisco

Asesor

Lambayeque, Mayo del 2015

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS

Tema:

‘‘Migración de IPv4 a IPv6 para mejorar la seguridad y velocidad de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo’’

TESIS DE GRADO

Aprobada ante el siguiente Jurado, para obtener el Título de:
INGENIERO ELECTRÓNICO

Ramírez Castro Manuel
Presidente del Jurado

Chiclayo Padilla Hugo
Secretario del Jurado

Romero Cortés Oscar Uchelly
Vocal del Jurado

Lambayeque, Mayo del 2015

AGRADECIMIENTO

A Dios por su infinita bondad y por habernos dado la oportunidad de haber hecho realidad esta tesis.

Al asesor de tesis Mg. Segundo Francisco Segura Altamirano por su constante apoyo y dedicación, quien con sus conocimientos, su experiencia y su paciencia ha logrado que podamos concluir esta tesis con éxito.

A nuestros familiares, amigos y a todas aquellas personas que de una u otra forma nos dieron su apoyo incondicional para hacer posible la presente tesis.

Tesistas

DEDICATORIA

A mi queridos padres Ausberto y Catalina por su motivación constante, sus sabios consejos y su amistad brindada.

A mi hermano Guillermo que es motivo de mi alegría cada día.

Robert Olivera Samamé

DEDICATORIA

Con inmenso cariño a mis padres Ricardo y Maritza por ser la razón de mi felicidad y estímulo para seguir adelante.

A mi hermano Ricardo por darme su apoyo incondicional para hacer realidad este sueño.

Cristian Manayay Ramírez

RESUMEN

Este proyecto de tesis fue realizado con la finalidad de conseguir una red más segura, más rápida y moderna, procediendo a migrar en forma gradual de IPv4 a IPv6, en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

La versión del protocolo enrutado IP que se utiliza actualmente y que se utilizó por mucho tiempo, por su gran poder y escalabilidad, fue el protocolo IPv4, pero desafortunadamente IPv4 quedó pequeño para todo el desarrollo y crecimiento de aplicaciones de las redes de computadoras que actualmente existen. Es por ello que la IETF decidió dar el paso como parte de la evolución misma de IP para llegar a su nueva versión la cual denominaron IPv6. Con IPv6, se aliviará toda la demanda naciente y creciente que se tiene hoy en día de direcciones IP, para cada una de las aplicaciones que se tienen y se tendrán en el futuro.

IPv6 ofrecerá poder direccionar 2^{128} nodos, lo que es equivalente a 340,282,366,920,938,463,374,607,431,768,211,456 nodos, debido a que ahora la dirección constará de 128 bits, lo cual elimina muchas de las herramientas que se utilizaban en IPv4 para poder optimizar el espacio de direccionamiento con el que se contaba 2^{32}.Y no solamente nos proporciona esta gran cantidad de host, sino también una mayor seguridad y un aumento de velocidad.

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

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

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

ABSTRACT

This thesis project was undertaken in order to achieve a safer, faster and modern network, proceeding gradually migrate from IPv4 to IPv6, in the Telematic Network of the National University Pedro Ruiz Gallo.

The version of IP routing protocol currently used and is used for long, for his great power and scalability, was the IPv4 protocol, IPv4 but unfortunately too small for the entire application development and growth of computer networks currently there. That is why the IETF decided to take the plunge as part of the evolution of IP to reach its new version which called IPv6. With IPv6, all new and growing demand that today has IP address will ease, for each of the applications that have and will have in the future.

IPv6 will offer to address 2 ^ 128 nodes, which is equivalent to 340,282,366,920,938,463,374,607,431,768,211,456 nodes, because now the direction consist of 128 bits, which eliminates many of the tools used in order to optimize the IPv4 address space with which 2 ^ 32.Y was counted not only provides us with this large amount of host, but also greater security and increased speed.

IPv6 brings a slight modification in the format of the header and in the means of addressing nodes. Now with IPv6, the fields will no longer be 8-bit fields represented in decimal form, but are fields of 16 bits represented in hexadecimal and are separated by ":", which changes the way of addressing and eliminating or changes some routing and management tools that were being used with IPv4.

In addition IPv6 requires other protocols in other layers to make changes to adapt to the new features IPv6 brings.

As safety is ensured that IETF IPsec it mandatory for IPv6, which allows all applications built much safer than those they had in IPv4. This adds IPsec security is added only to the Internet layer, and can predict that based on the lessons learned with IPv4, regarding security, IPv6 is more secure than IPv4.

INTRODUCCIÓN

La IETF decidió desarrollar un nuevo protocolo, que no es más que una evolución de IPv4, el cual le denominaron IPv6 o IPng. Con éste nuevo protocolo IPv6, el problema de direccionamiento queda resuelto y a su vez mejora en gran manera la seguridad de la red y velocidad de la misma.

En éste proyecto de tesis se realizará una introducción a las redes, así como de un análisis detallado del protocolo actual IPv4. También se analizará las características del nuevo protocolo IPv6, y en base a esto y al anterior análisis poder determinar cuáles son los beneficios y bondades de IPv6.

También se conocerá la realidad de la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, posteriormente se procederá a una simulación del diseño de la Red Telemática con Packet Tracer, usando el Dual Stack como estrategia de migración paulatina entre ambos protocolos (IPv4 con IPv6).

ÍNDICE

CAPÍTULO I

PROBLEMÁTICA

I. PROBLEMÁTICA

1.1. Objetivos

1.1.1. Objetivo General

Migrar en forma gradual de IPv4 a IPv6, en la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo.

1.1.2. Objetivos Específicos

- Estudiar la realidad actual de la red telemática de la UNPRG.
- Evaluar y probar las ventajas de la IPv4 e IPv6 en una red de prueba.
- Establecer un plan de Migración de una red de prueba y evaluar el desempeño.
- Verificar la rapidez y seguridad de la red con IPv6.

1.2. Justificación e Importancia

La presente Tesis se justifica en los siguientes aspectos:

- Tecnológicamente, la tesis propone el diseño de la Red y su respectiva aplicación, y contribuirá al desarrollo tecnológico en la Red Telemática, permitiéndoles que tengan una red más segura, más rápida y moderna.
- Institucionalmente, el trabajo de investigación beneficiará directamente al cuerpo de trabajadores de la Red telemática, a los catedráticos y a los estudiantes de la UNPRG por cuanto mejorará el rendimiento de la red y la respectiva seguridad de la información que se maneje y por ende se brindará un mejor servicio a terceros.

1.3. Árbol de Problemas

1.3.1. Planteamiento del Problema

En la actualidad, la red telemática de la Universidad Nacional Pedro Ruiz Gallo usa IPv4 como protocolo de red para el intercambio de datos. El principal problema de este protocolo es el agotamiento de sus direcciones, etiquetas que

identifican de manera lógica las interfaces entre las que se realiza la comunicación; de los cuales, los últimos bloques están siendo asignados por los diferentes Registros Regionales de Internet (RIR por sus siglas en inglés) y éstos a su vez comunican el agotamiento inminente de direcciones y la necesidad de migrar a la versión 6 del protocolo IP para continuar con la satisfacción de la demanda de dominios en un mundo en el que las comunicaciones son de vital importancia.[NEWS, 20, pag, 10]

Entre otra de las de ciencias de IPv4 existe la falta de seguridad integrada en dicho protocolo, dado que IPv4 fue definido con la RFC791 en 1981, donde la seguridad era considerada opcional y algunos factores ya no se ajustan a las amenazas existentes en estos días.[Postel, 1981]

Por las razones antes mencionadas, en algún momento todas las redes del mundo se verán obligadas a migrar de forma paulatina a IPv6 para asegurar su conectividad.

1.3.2. Formulación del problema científico

¿De qué manera la migración de IPv4 a IPv6 mejora la velocidad y seguridad de la Red Telemática de la universidad nacional Pedro Ruiz Gallo?

CAPÍTULO II

INTRODUCIÓN A LAS REDES

II. INTRODUCIÓN A LAS REDES

Actualmente las redes de computadoras desempeñan un papel importante en el desarrollo de las comunicaciones. Esto se puede observar claramente en aquel estudiante que necesita descargar un archivo para terminar su tarea o en el gerente que necesita establecer una videoconferencia con su homólogo en la sede de Colombia pues sus limitantes son la distancia y el tiempo. Se ha podido observar, de acuerdo a los últimos avances, que las telecomunicaciones están estrechamente relacionadas con las redes computadoras, pues ahora desde muchos teléfonos móviles, se puede acceder a un computador servidor, y de éste poder descargar aplicaciones para el móvil, o poder enviar correos electrónicos que son almacenados en un servidor.

2.1. Redes de datos

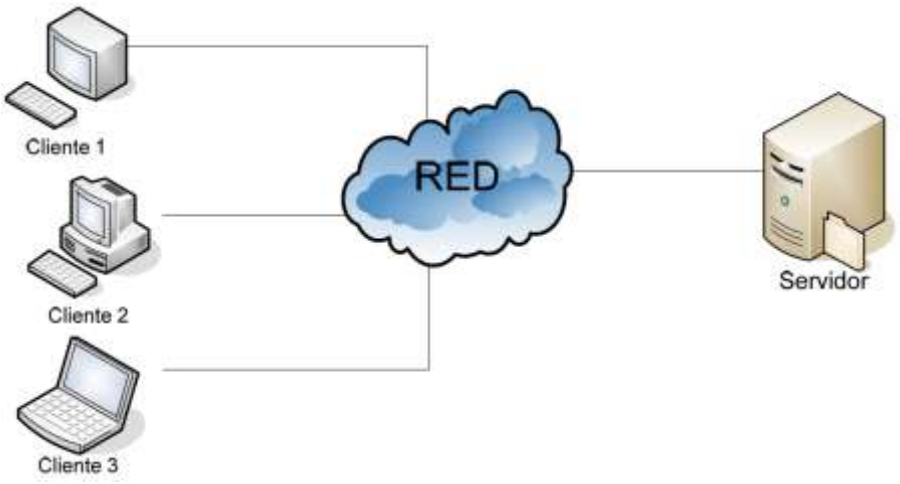
Se conoce como red de datos a la infraestructura cuyo diseño posibilita la transmisión de información a través del intercambio de datos, la cual se puede modificar y actualizar de manera rápida y eficaz, y a su vez reducir los costos de la empresa. [Tanenbaum and Wetherall, Computer Networks, 2011].

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

Los modelos de comunicación entre computadoras que existen en las redes son, el modelo cliente-servidor y el modelo igual-igual.

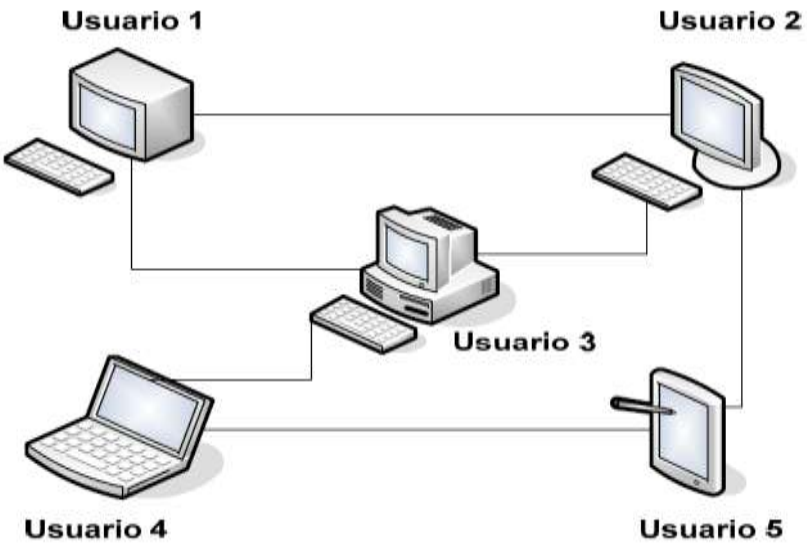
El modelo cliente-servidor es el más utilizado en la redes actuales, pues es aplicable para distancias cortas y para distancias largas. En este modelo existe un servidor, que es una computadora bastante poderosa donde están almacenados todos los datos, y los clientes son las computadoras sencillas que los usuarios tienen en sus oficinas. [Tanenbaum and Wetherall, Computer Networks, 2011] ***(Ver Imagen N° 01)***

Imagen N° 01: Modelo Cliente – Servidor



En el modelo igual-igual cada usuario de un grupo en particular puede comunicarse con una o más personas del grupo, el término cliente y servidor es relativo, pues se considera a cliente a aquella máquina que está haciendo la petición de un archivo y a servidor a aquella que le entrega el archivo a la primera. [Tanenbaum and Wetherall, Computer Networks, 2011]. **(Ver Imagen N° 02)**

Imagen N° 02: Modelo Igual – Igual



2.1.1. Topología de la red

La topología de red define la estructura de una red. Una parte de la definición topológica es la topología física, que es la disposición real de los cables o medios. La otra parte es la topología lógica, que define la forma en que los hosts acceden a los medios para enviar datos. [CCNA1, Módulo2]. ***(Ver Imagen N° 03)***

Imagen N° 03: Topologías físicas

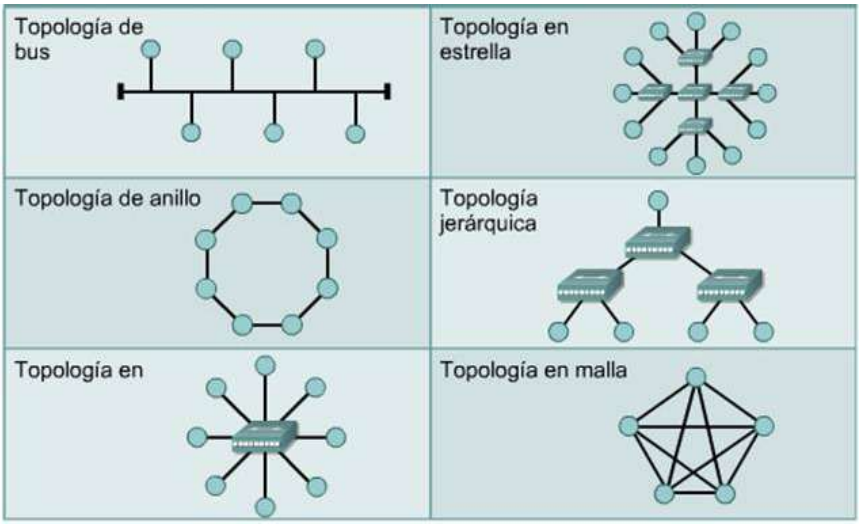
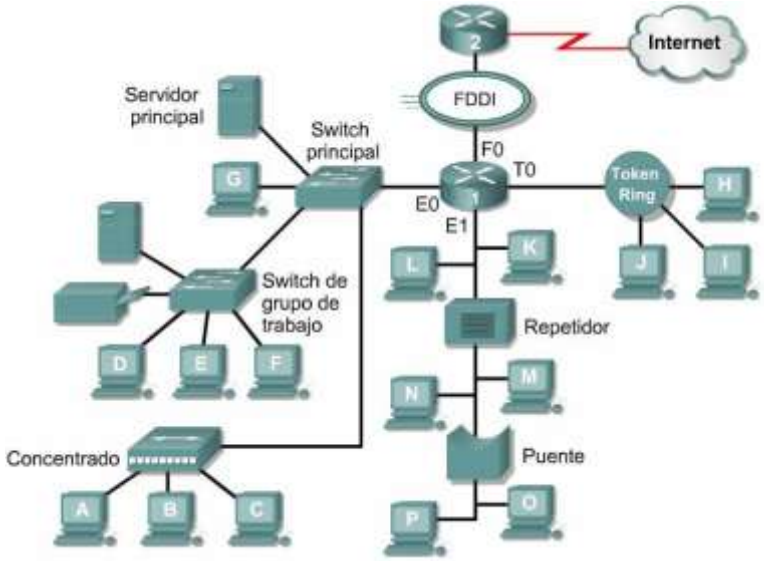


Imagen N° 04: Ejemplo de topología



1. Una topología de bus usa un solo cable backbone que debe terminarse en ambos extremos. Todos los hosts se conectan directamente a este backbone.

2. La topología de anillo conecta un host con el siguiente y al último host con el primero. Esto crea un anillo físico de cable.

3. La topología en estrella conecta todos los cables con un punto central de concentración.

4. Una topología en estrella extendida conecta estrellas individuales entre sí mediante la conexión de hubs o switches. Esta topología puede extender el alcance y la cobertura de la red.

5. Una topología jerárquica es similar a una estrella extendida. Pero en lugar de conectar los hubs o switches entre sí, el sistema se conecta con un computador que controla el tráfico de la topología.

6. La topología de malla se implementa para proporcionar la mayor protección posible para evitar una interrupción del servicio. El uso de una topología de malla en los sistemas de control en red de una planta nuclear sería un ejemplo excelente. Como se puede observar en el gráfico, cada host tiene sus propias conexiones con los demás hosts. Aunque la Internet cuenta con múltiples rutas hacia cualquier ubicación, no adopta la topología de malla completa.

La topología lógica de una red es la forma en que los hosts se comunican a través del medio. Los dos tipos más comunes de topologías lógicas son broadcast y transmisión de tokens.

La topología broadcast simplemente significa que cada host envía sus datos hacia todos los demás hosts del medio de red. No existe una orden que las estaciones deban seguir para utilizar la red. Es por orden de llegada. Ethernet funciona así, tal como se explicará en el curso más adelante.

La segunda topología lógica es la transmisión de tokens. La transmisión de tokens controla el acceso a la red mediante la transmisión de un token electrónico a cada host de forma secuencial. Cuando un host recibe el token, ese host puede enviar datos a través de la red. Si el host no tiene ningún dato para enviar, transmite el token al siguiente host y el proceso se vuelve a repetir. Dos ejemplos de redes que utilizan la transmisión de tokens son Token Ring y la Interfaz de datos distribuida por fibra (FDDI). Arcnet es una variación de Token Ring y FDDI. Arcnet es la transmisión de tokens en una topología de bus.

2.1.2. Clasificación de las Redes según se Extensión Geográfica

Según su extensión geográfica las redes de computadoras se pueden clasificar en:

2.1.2.1. Red de Área Local

La palabra LAN se deriva de las siglas en inglés *Local Area Network* que en español significa red de área local. Son redes de propiedad privada que se encuentran en un solo edificio o en un campus de pocos kilómetros de longitud.

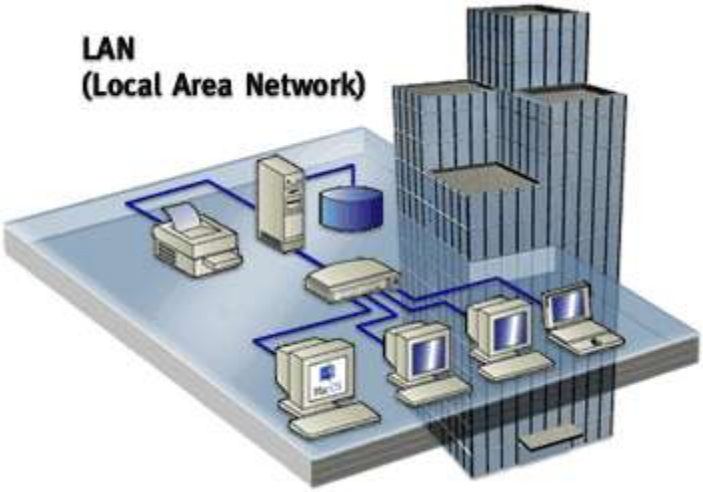
Se utilizan ampliamente para conectar computadoras personales y estaciones de trabajo en oficinas de una empresa y de fábricas para compartir recursos (por ejemplo, impresoras) e intercambiar información.

Las LANs son diferentes de otros tipos de redes en tres aspectos: 1) tamaño; 2) tecnología de transmisión, y 3) topología. Las LANs están restringidas por tamaño, es decir, el tiempo de transmisión en el peor de los casos es limitado y conocido de antemano. El hecho de conocer este límite permite utilizar ciertos tipos de diseño, lo cual no sería posible de otra manera. Esto también simplifica la administración de la red.

Las LANs podrían utilizar una tecnología de transmisión que consiste en un cable al cual están unidas todas las máquinas, como alguna vez lo estuvo parte de las líneas de las compañías telefónicas en áreas rurales. Las LANs tradicionales se ejecutan a una velocidad de 10 a 100 Mbps, tienen un retardo bajo (microsegundos o nanosegundos) y cometen muy pocos errores.

Las LANs más nuevas funcionan hasta a 10 Gbps. [Tanenbaum and Wetherall, Computer Networks, 2011]. **(Ver Imagen N° 05)**

Imagen N° 05: Red de área local



Algunas de las tecnologías comunes de LAN son: Ethernet, Token Ring, FDDI.

2.1.2.2. Red de Área Metropolitana

A este tipo de red también se le conoce como MAN, de sus siglas en inglés, *Metropolitan Area Network*, que traducidas a español significan Red de Área Metropolitana.

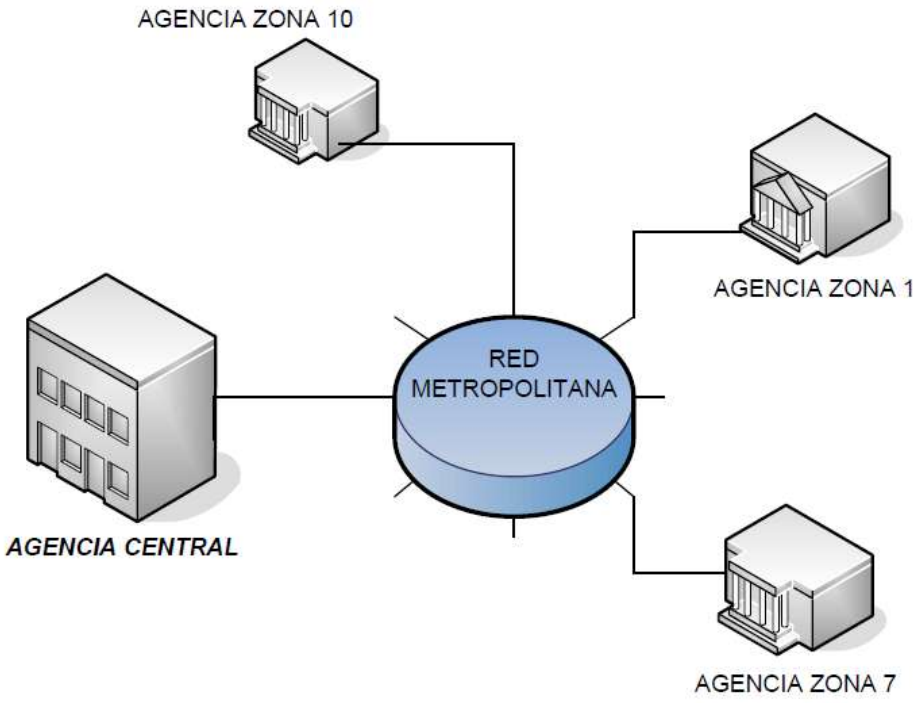
Una red de área metropolitana (MAN) abarca una ciudad. El ejemplo más conocido de una MAN es la red de televisión por cable disponible en muchas ciudades.

Una MAN consta generalmente de dos o más LAN dentro de un área geográfica común. Una MAN puede abarcar un área geográfica equivalente a una ciudad, o aproximadamente 10 kilómetros entre procesadores. Continuando con el ejemplo de las agencias bancarias, se puede considerar a una MAN como la red que se forma cuando interconectamos a todas las

agencias dentro de la ciudad y todas teniendo comunicación con la agencia central.

Por ejemplo, un banco con varias sucursales puede utilizar una MAN. Normalmente, se utiliza un proveedor de servicios para conectar dos o más sitios LAN utilizando líneas privadas de comunicación o servicios ópticos. También se puede crear una MAN usando tecnologías de puente inalámbrico enviando haces de luz a través de áreas públicas. [Tanenbaum and Wetherall, Computer Networks, 2011]. **(Ver Imagen N° 06)**

Imagen N° 06: Red de área metropolitana



2.1.2.3. Red de Área Extensa

A este tipo de red también se le conoce como WAN, por sus siglas en inglés, Wide Area Network, que traducidas significan red de área amplia o extensa. Las redes de área amplia se utilizan para interconectar las redes LAN. Se les denomina redes de área amplia, pues las longitudes que recorren los cableados entre un dispositivo y otro son más de un kilómetro, a diferencia de una red de área local que el cableado tiene como longitud máxima 1000

metros entre procesadores. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes. Una WAN está diseñada para operar entre área geográfica extensas, ofrecer recursos remotos de tiempo completo y en tiempo real, conectado a servicios locales. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

Esta red se extiende por una amplia zona geográfica, a menudo un país o continente; un ejemplo es una empresa con sucursales en diferentes ciudades. [Tanenbaum and Wetherall, Computer Networks, 2011].

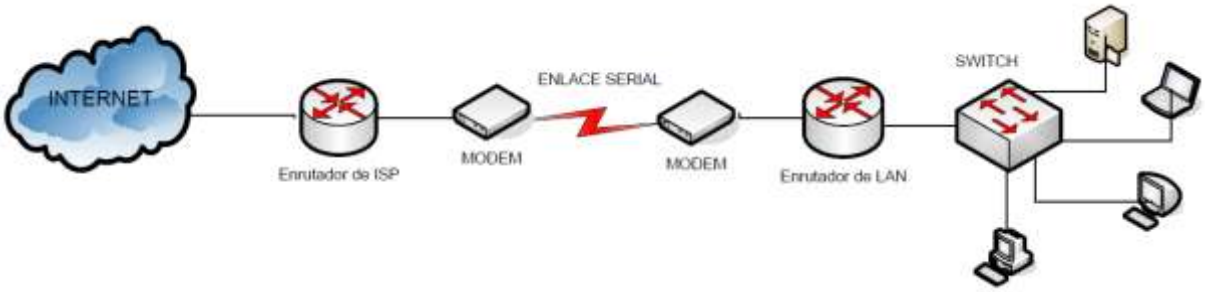
Las WAN interconectan las LAN, que a su vez proporcionan acceso a los computadores o a los servidores de archivos ubicados en otros lugares. Como las WAN conectan redes de usuarios dentro de un área geográfica extensa, permiten que las empresas se comuniquen entre sí a través de grandes distancias. Las WAN permiten que los computadores, impresoras y otros dispositivos de una LAN compartan y sean compartidas por redes en sitios distantes. Las WAN proporcionan comunicaciones instantáneas a través de zonas geográficas extensas. El software de colaboración brinda acceso a información en tiempo real y recursos que permiten realizar reuniones entre personas separadas por largas distancias, en lugar de hacerlas en persona. [CCNA1, Módulo 1]

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

Una red de área amplia o extendida es la que se forma por un enrutador, al cual están conectados todos los hosts de una LAN, y el enrutador del proveedor de servicio de Internet o ISP (Internet Service Provider). El tipo de enlace que existe entre el enrutador del cliente y el enrutador del ISP utiliza una interface serial, a diferencia de una LAN que utiliza una interface Ethernet o FastEthernet, dependiendo de la configuración de la velocidad de ésta. **(Ver Imagen N° 06)**

Imagen N° 06: Diseño de una Red de Área Extensa

.



Se observa una WAN en la cual se conecta por medio de un enlace serial, toda una LAN hacia la nube de Internet. No necesariamente tiene que conectarse a Internet, sino que también se podría utilizar una WAN para interconectar dos LAN remotas que estén separadas por una gran distancia. En los enlaces WAN se habla del tipo de encapsulamiento para establecer la comunicación.

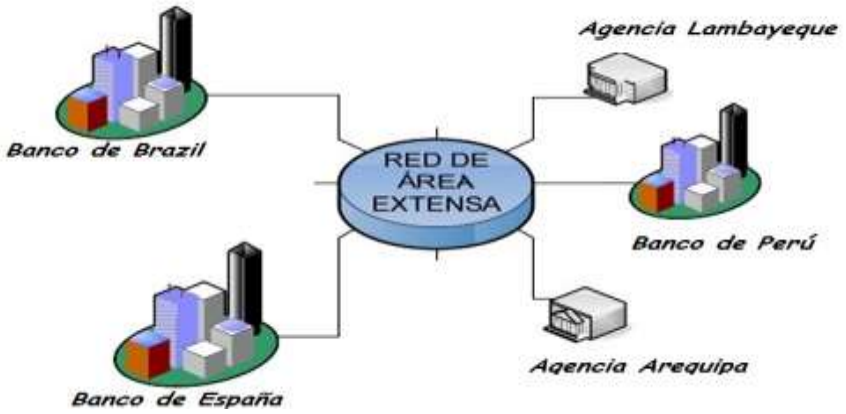
Los tipos de encapsulamientos pueden ser:

- PPP (Point to point protocol o protocolo de punto a punto)
- HDLC (Control de enlace de datos de alto nivel)

Una WAN puede abarcar un país, un continente e incluso un planeta. Esto quiere decir que se puede considerar Internet como una red WAN, pues ésta abarca todo el planeta.

Ejemplo: Se puede decir que una WAN es la que se construye cuando unimos por medio de enlaces las agencias de todo el país de Perú, y establecemos enlaces con otras agencias en el interior de Perú y con bancos de otros países. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009] **(Ver Imagen N° 07)**

Imagen N° 07: Red de Área Extensa



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

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

Los enrutadores se pueden utilizar en una LAN, pero su uso es diferente, pues en este tipo de red se utiliza para aumentar los dominios de broadcast o sea para segmentar una red y con ello obtener subredes. En una WAN sus funciones principales son, elegir la mejor ruta para enviar los paquetes y la de conmutación de los paquetes a la interfaz correcta. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

Todos los estándares WAN son definidos por varias autoridades, como:

- Fuerza de Tareas de Ingeniería de Internet (IETF)

- Organización Internacional de Normalización (ISO)
- Sector de Normalización de Telecomunicaciones de la Unión Internacional de Telecomunicaciones (UIT-T)
- Asociación de Industrias Electrónicas (EIA)

2.2. Modelos de Capas y Protocolos

2.2.1. Modelos de Referencia OSI

Las siglas OSI provienen de los términos en inglés *Open System Interconnection o Interconexión de sistemas abiertos*, pues es un modelo que como su nombre lo indica, nos sirve como referencia para otros modelos.

ISO desarrolló un modelo de red. Dado que la comunicación entre una estación y otra estación es un proceso que si se ve como uno solo, sería muy complejo de poder entender cómo funciona. Es por ello que se establecen capas para poder entender de una mejor manera como se establece paso a paso la comunicación entre estaciones. [Peterson and Davie, 2011].

El modelo OSI es un modelo de referencia propuesto por la ISO (Organización Internacional de Estándares) como resultado de la necesidad de ayudar a los fabricantes a crear redes que sean compatibles con otras redes (tener un estándar para los distintos protocolos) que a principios de los años 80 comenzaron a crecer rápidamente. [Peterson and Davie, 2011].

El modelo OSI fue lanzado en el año 1984 y proporcionó a los fabricantes un conjunto de estándares que aseguraron una mayor compatibilidad entre los distintos tipos de tecnología de red. El modelo OSI es un modelo que tiene 7 capas, las cuales van desde el medio físico por el que se transmiten los datos, hasta la parte de las aplicaciones, que son con las cuales el usuario tiene interactividad. [Peterson and Davie, 2011].

2.2.1.1. Ventajas del Modelo OSI

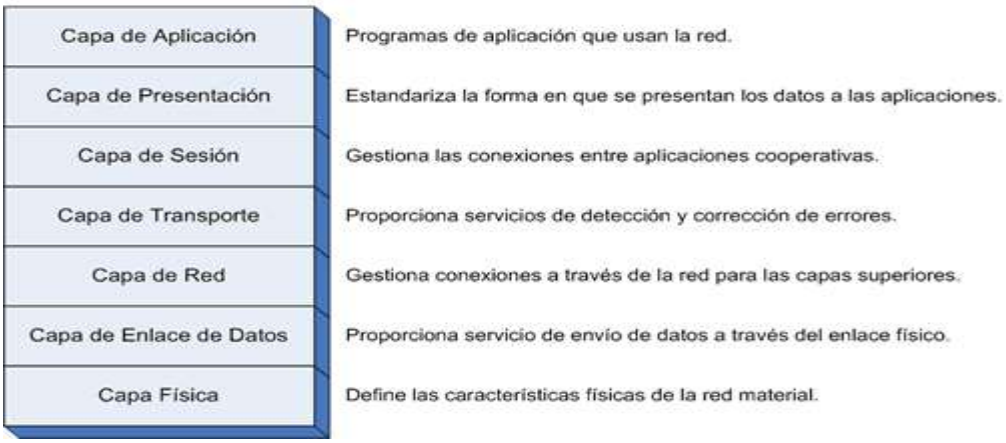
- Reduce la velocidad
- Estandariza las interfaces
- Facilita el diseño modular

- Asegura la interoperabilidad de la tecnología
- Acelera la evolución
- Simplifica la enseñanza y el aprendizaje

El modelo de referencia OSI se ha convertido en el modelo principal para las comunicaciones por red. Aunque existen otros modelos, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia de OSI. Esto es en particular así cuando lo que buscan es enseñar a los usuarios a utilizar sus productos. Se considera la mejor herramienta disponible para enseñar cómo enviar y recibir datos a través de una red.

2.2.1.2. Capas del modelo OSI

Imagen N° 08: Capas del Modelo OSI

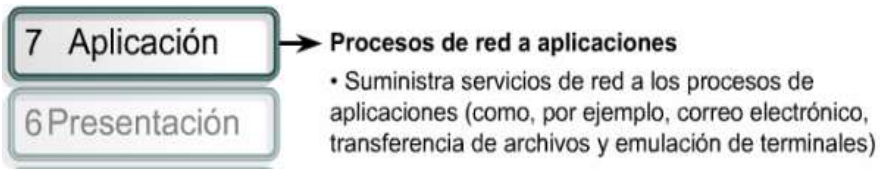


2.2.1.2.1. Capa de Aplicación

Se utiliza para intercambiar los datos entre los programas que se ejecutan en los host de origen y destino). Proporciona la interfaz y servicios q soportan las aplicaciones de usuario. También se encarga de ofrecer acceso general a la red.
Esta capa suministra las herramientas q el usuario, de hecho ve. También ofrece los servicios de red relacionados con estas aplicaciones, como la gestión de mensajes, la transferencia de archivos y las consultas a base de datos. Entre los servicios de intercambio de información q gestiona la capa de

aplicación se encuentran los protocolos SMTP, Telnet, FTP, HTTP. [Peterson and Davie, 2011].

Imagen N° 09: Capa de Aplicación

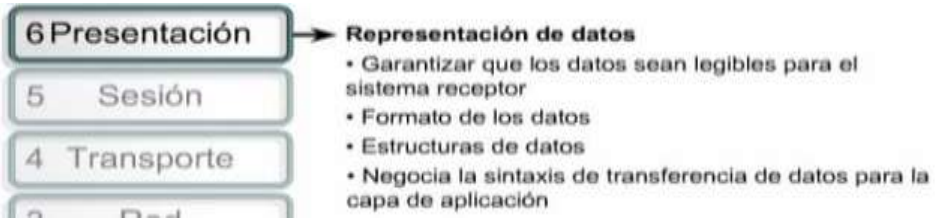


2.2.1.2.2. Capa de Presentación

Codifica y convierte los datos de la Capa de Aplicación, también encripta los datos para transmisión y descifre de ellos cuando se reciben en el destino.

La capa de presentación puede considerarse el traductor del modelo OSI. Esta capa toma los paquetes de la capa de aplicación y los convierte a un formato genérico que pueden leer todas las computadoras. Par ejemplo, los datos escritos en caracteres ASCII se traducirán a un formato más básico y genérico. También se encarga de cifrar los datos así como de comprimirlos para reducir su tamaño. El paquete que crea la capa de presentación contiene los datos prácticamente con el formato con el que viajaran por las restantes capas de la pila OSI (aunque las capas siguientes Irán añadiendo elementos al paquete. [Universidad privada cumbre, Redes I].

Imagen N° 10: Capa de Presentación

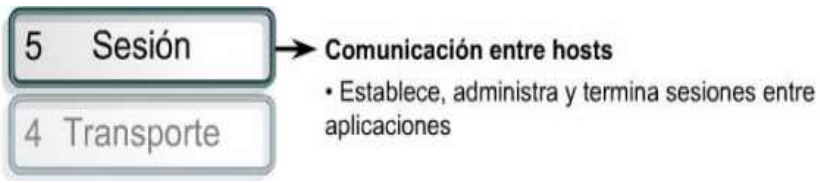


2.2.1.2.3. Capa de Sesión

Se encarga de Crear y mantener diálogos entre las aplicaciones de origen y destino, también maneja el intercambio de información para iniciar diálogos y mantener los activos.

La capa de sesión es la encargada de establecer el enlace de comunicación o sesión y también de finalizarla entre las computadoras emisora y receptora. Esta capa también gestiona la sesión que se establece entre ambos nodos La capa de sesión pasa a encargarse de ubicar puntas de control en la secuencia de datos además proporciona cierta tolerancia a fallos dentro de la sesión de comunicación
Los protocolos que operan en la capa de sesión pueden proporcionar dos tipos distintos de enfoques para que los datos vayan del emisor al receptor: la comunicación orientada a la conexión y la comunicación sin conexión
Los protocolos orientados a la conexión que operan en la capa de sesi6n proporcionan un entorno donde las computadoras conectadas se ponen de acuerdo sobre los parámetros relativos a la creación de los puntos de control en los datos, mantienen un dialogo durante la transferencia de los mismos, y después terminan de forma simultanea la sesión de transferencia. [Universidad privada cumbre, Redes I].

Imagen N° 11: Capa de Sesión

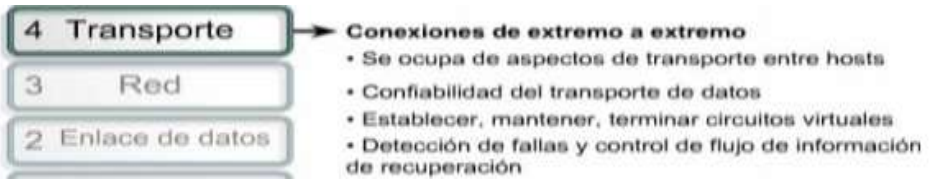


2.2.1.2.4. Capa de Transporte

Prepara los datos de la aplicación para el transporte a través de la red y procesa los datos de la red para su utilización por parte de las aplicaciones. La capa de transporte es la encargada de controlar el flujo de datos entre los nodos que establecen una comunicación; los datos no solo deben entregarse sin errores, sino además en la secuencia que proceda. La capa de transporte se ocupa también de evaluar el tamaño de los paquetes con el fin de que estos Tengan el tamaño requerido por las capas inferiores del conjunto de protocolos. El tamaño

de los paquetes 10 dicta la arquitectura de red que se utilice. [Universidad privada cumbre, Redes I].

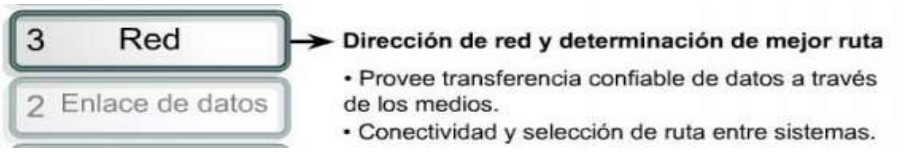
Imagen N° 12: Capa de Transporte



2.2.1.2.5. Capa de Red

La capa de red encamina los paquetes además de ocuparse de entregarlos. La determinación de la ruta que deben seguir los datos se produce en esta capa, lo mismo que el intercambio efectivo de los mismos dentro de dicha ruta, La Capa 3 es donde las direcciones lógicas (como las direcciones IP de una computadora de red) pasan a convertirse en direcciones físicas (las direcciones de hardware de la NIC, la Tarjeta de Interfaz para Red, para esa computadora especifica).
Los routers operan precisamente en la capa de red y utilizan los protocolos de encaminamiento de la Capa 3 para determinar la ruta que deben seguir los paquetes de datos. [Universidad privada cumbre, Redes I].

Imagen N° 13: Capa de Red

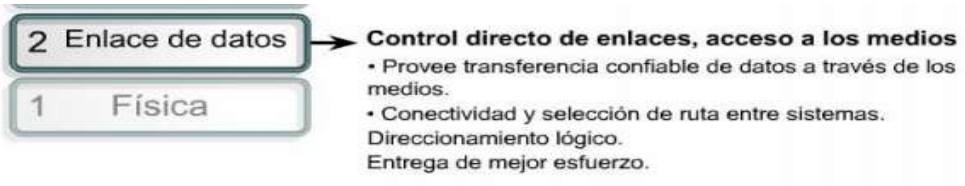


2.2.1.2.6. Capa de Enlace de Datos

Cuando los paquetes de datos llegan a la capa de enlace de datos, estas pasan a ubicarse en tramas (unidades de datos), que vienen definidas por la arquitectura de red que se está utilizando (como Ethernet, Token Ring, etc.). La capa de enlace de datos se encarga de desplazar los datos por el enlace físico de comunicación hasta el nodo receptor, e identifica cada computadora incluida

en la red de acuerdo con su dirección de hardware La información de encabezamiento se añade a cada trama que contenga las direcciones de envío y recepción. La capa de enlace de datos también se asegura de que las tramas enviadas por el enlace físico se reciben sin error alguno. Por ello, los protocolos que operan en esta capa adjuntaran un Chequeo de Redundancia Cíclica (Cyclical Redundancy Check a CRC) al final de cada trama. EI CRC es básicamente un valor que se calcula tanto en la computadora emisora como en la receptora, Si los dos valores CRC coinciden, significa que la trama se recibió correcta e íntegramente, y no sufrió error alguno durante su transferencia. [Universidad privada cumbre, Redes I].

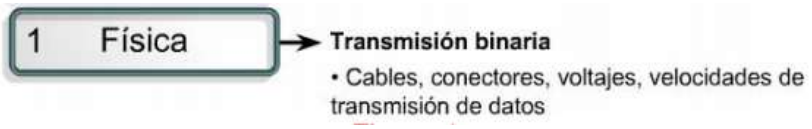
Imagen N° 14: Capa de Enlace de Datos



2.2.1.2.7. Capa Física

En la capa física las tramas procedentes de la capa de enlace de datos se convierten en una secuencia única de bits que puede transmitirse por el entorno físico de la red. La capa física también determina los aspectos físicos sobre la forma en que el cableado está enganchado a la NIC de la computadora. [Universidad privada cumbre, Redes I].

Imagen N° 15: Capa Física



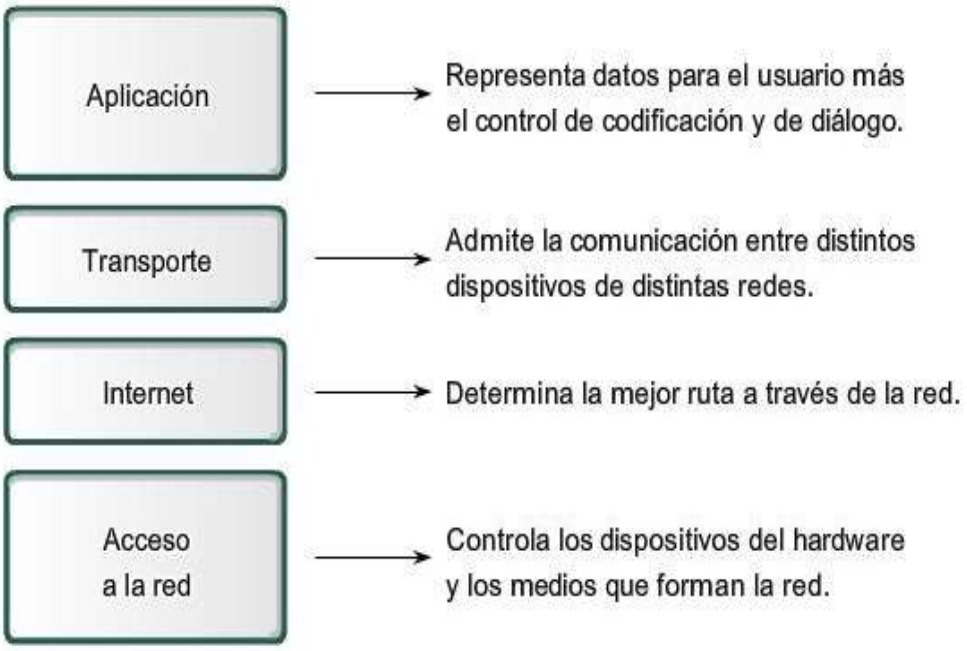
2.2.2. Modelo TCP/IP

El estándar histórico y técnico de la Internet es el modelo TCP/IP. El Departamento de Defensa de EE.UU. (DoD) creó el modelo de referencia TCP/IP porque necesitaba diseñar una red que pudiera sobrevivir ante cualquier

circunstancia, incluso una guerra nuclear. En un mundo conectado por diferentes tipos de medios de comunicación, como alambres de cobre, microondas, fibras ópticas y enlaces satelitales, el DoD quería que la transmisión de paquetes se realizara cada vez que se iniciaba y bajo cualquier circunstancia. Este difícil problema de diseño dio origen a la creación del modelo TCP/IP.

El TCP/IP se desarrolló como un estándar abierto. Esto significaba que cualquier persona podía usar el TCP/IP. Esto contribuyó a acelerar el desarrollo de TCP/IP como un estándar. El modelo TCP/IP tiene las siguientes cuatro capas. [CCNA1, módulo2]

Imagen N° 16: Capas del modelo TCP/IP



Algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta. Lo más notable es que la capa de aplicación posee funciones diferentes en cada modelo. Los diseñadores de TCP/IP sintieron que la capa de aplicación debía incluir los detalles de las capas de sesión y presentación OSI. Crearon una capa de aplicación que maneja aspectos de representación, codificación y control de diálogo. [CCNA1,Módulo2]

2.2.2.1. Capas del modelo TCP/IP

2.2.2.1.1. Capa de acceso a la red

La primera capa es la capa de acceso a la red o también denominada host a red. Esta capa se encarga del intercambio de datos entre una estación y la red y entre los dispositivos de la misma red. En esta capa se incluyen los detalles de la tecnología LAN y WAN que utiliza la red. Esta capa define los procedimientos para realizar la interfaz con el hardware de la red y para poder obtener acceso al medio de transmisión físico. Como su nombre lo indica en esta capa se definen todos los procedimientos para que una estación pueda acceder a la red, además se definen las direcciones físicas o direcciones MAC que serán utilizadas por la capa Internet para asociarla a una dirección lógica o dirección IP. La capa física y de enlace de datos del modelo OSI son comprendidas en la capa de acceso a la red y todas las características que se explicaron anteriormente para estas dos capas del modelo OSI describen también a esta capa. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

2.2.2.1.2. Capa de Internet

La segunda capa del modelo TCP/IP es la capa de Internet, esta capa al igual que la capa de red del modelo OSI, su propósito es escoger la mejor ruta para poder encaminar un paquete a través de todas las redes que estén en el camino desde la estación origen hasta la estación destino. Además esta capa provee el direccionamiento lógico o dirección IP que se asigna a cada estación la cual es utilizada por los protocolos de capas superiores para poder identificar a que estación destino enviarán los datos y a que red pertenecen. El protocolo de resolución de direcciones (ARP) permite que el protocolo enrutado IP identifique la dirección física que corresponde a una dirección lógica IP. Los protocolos principales que operan en esta capa son el protocolo enrutado IP (Internet Protocol), ARP, ICMP (Internet Control Message Protocol o protocolo de Internet de control de mensaje) que es el responsable de proveer diagnósticos de funciones y reportar errores en la entrega, pero no corrige errores, e IGMP (Internet Group Managment Protocol o protocolo de Internet de manejo de grupo) que es el responsable del manejo de grupo de multicast o multitransmisión. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

2.2.2.1.3. Capa de Transporte

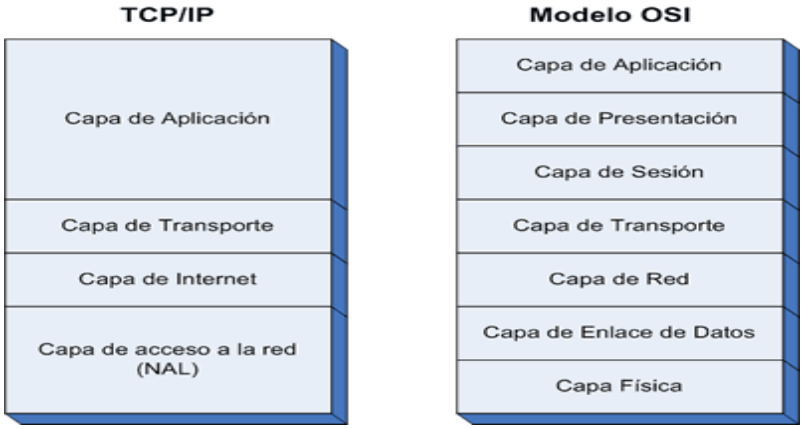
La capa 3 del modelo TCP/IP es la capa de transporte, tiene las mismas funciones que la capa de transporte del modelo OSI anteriormente explicada. A esta capa también se le conoce como capa de host a host. La capa de transporte es la responsable de proveer las herramientas para que los paquetes sean transmitidos desde una estación origen a una estación destino. En esta capa los paquetes de capa 2 se encapsulan y se les agrega una cabecera para formar lo que es un segmento. La capa de transporte lleva un control de cada segmento transmitido y dependiendo de que protocolo se utilice puede corregir los errores y retransmitir segmentos que no llegaron o llegaron corrompidos a su destino. Además esta capa ofrece el control de flujo, con lo cual el host destino le dice al host origen que envíe más lento o más rápido los segmentos. Los protocolos que trabajan en esta capa son el protocolo de control de transmisión (TCP) y el protocolo de datagrama de usuario (UDP). [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

2.2.2.1.4. Capa de Aplicación

La última capa del modelo TCP/IP es la capa de aplicación. En esta capa al igual que en el modelo OSI, se encuentran las aplicaciones que no son más que las interfaces para acceder a los servicios de las demás capas inferiores. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

2.2.3. Comparación entre el modelo OSI con el modelo TCP/IP

Imagen N° 17: Comparación entre el modelo OSI con el modelo TCP/IP



2.2.3.1. Las similitudes incluyen:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Ambos modelos deben ser conocidos por los profesionales
- Ambos suponen que se conmutan paquetes. Esto significa que los paquetes individuales pueden usar rutas diferentes para llegar al mismo destino. Esto se contrasta con las redes conmutadas por circuito, en las que todos los paquetes toman la misma ruta.

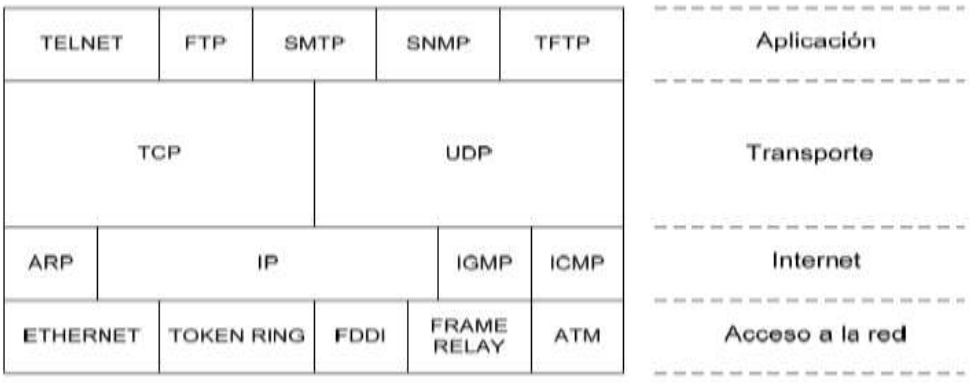
2.2.3.2. Las diferencias incluyen:

- TCP/IP combina las funciones de la capa de presentación y de sesión en la capa de aplicación.
- TCP/IP combina la capa de enlace de datos y la capa física del modelo OSI en la capa de acceso de red.
- TCP/IP parece ser más simple porque tiene menos capas.
- Los protocolos TCP/IP son los estándares en torno a los cuales se desarrolló la Internet, de modo que la credibilidad del modelo TCP/IP se debe en gran parte a sus protocolos. En comparación, por lo general las redes no se desarrollan a partir del protocolo OSI, aunque el modelo OSI se usa como guía.

2.2.2.2. Principales protocolos del conjunto TCP/IP

El modelo TCP/IP es un conjunto de varios protocolos que trabajan en diferentes capas, de todos estos protocolos los que más sobresalen y que más se utilizan son el IP de capa 3 OSI y el protocolo orientado a conexión TCP, de aquí el nombre TCP/IP. También podría existir la combinación UDP/IP o TCP/IPX por ejemplo en cada capa del modelo TCP/IP trabajan ciertos protocolos y aplicaciones, algunos de ellos son: [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

Imagen N° 18: Arquitectura de protocolos de TCP/IP



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

CAPÍTULO III

ANÁLISIS DEL PROTOCOLO IPv4

III. ANÁLISIS DEL PROTOCOLO IPv4

IP o protocolo de Internet es un protocolo no orientado a conexión, poco confiable que su principal función es el direccionamiento y crear paquetes que puedan ser encaminados entre estaciones.

No orientado a conexión significa que la conexión no es establecida antes de comenzar a transmitir datos. Poco confiable se refiere a que la entrega de los paquetes no es garantizada, estos trabajos son responsabilidad de las capas superiores y por ello IP no lo ejecuta. La versión de este protocolo que se está utilizando actualmente es la versión 4, de ahí que su nombre resumido sea IPv4. Esta versión es especificada en el RFC 791 publicada en Septiembre de 1981 y que está basado en 6 ediciones anteriores, esto quiere decir que este RFC es una actualización de 6 anteriores. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

3.1. Características de IPv4

3.1.1. Formato de cabecera de un paquete IPv4

El formato de la cabecera de un paquete IP o datagrama versión 4 se ilustra en la figura se puede observar cada uno de los campos que conforma dicha cabecera. **(Ver Imagen N° 19 y N° 20)**

Imagen N° 19: [RFC-791], Formato de cabecera de un paquete IPv4-N°01

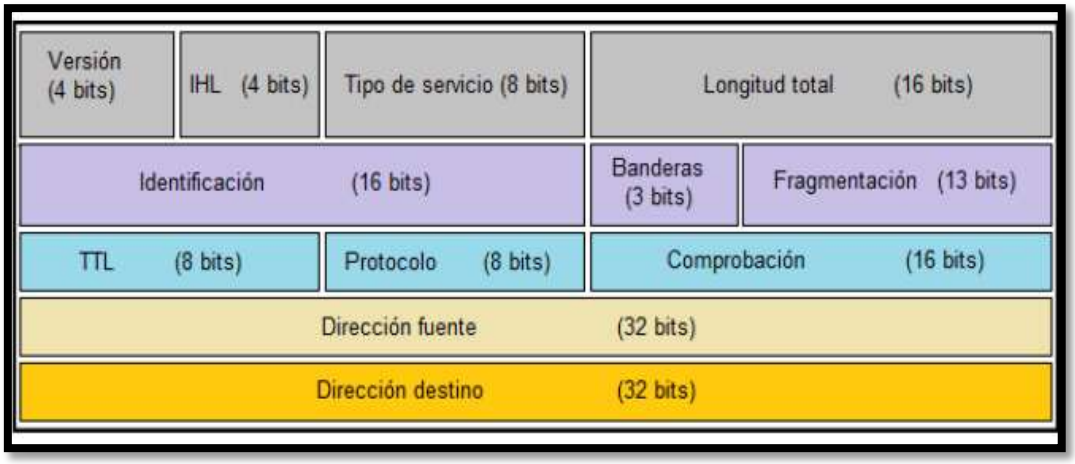
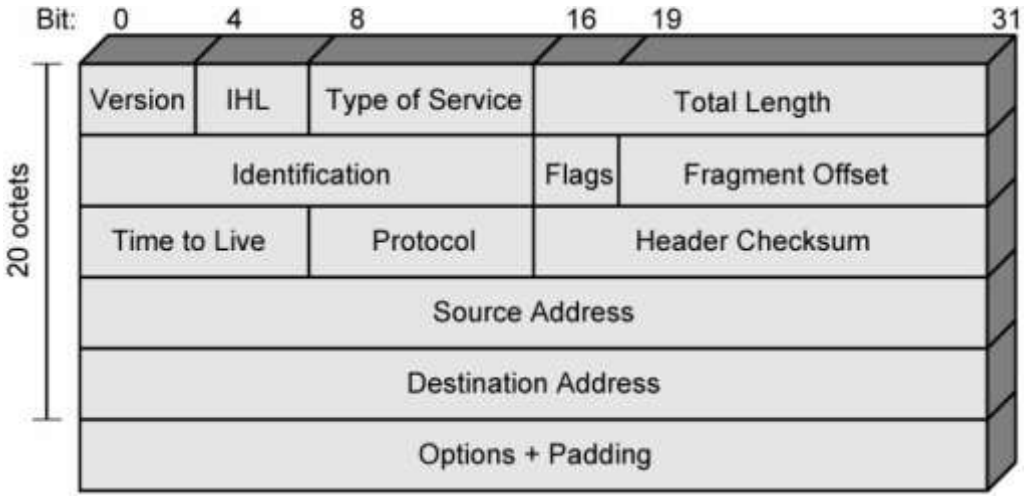


Imagen N° 20: Formato de cabecera de un paquete IPv4-N°02



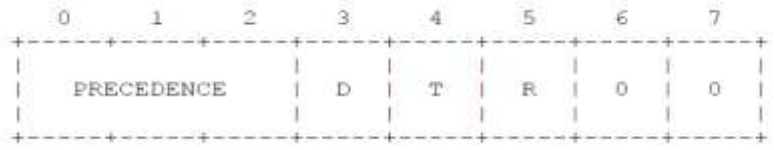
- El primer campo que presenta esta cabecera es el campo de versión e indica el formato o versión que la cabecera está utilizando, este campo está compuesto por 4 bits. En la actualidad este campo indica la versión 4 en la mayoría de redes. Las redes que ya están utilizando IP versión 6, deben de tener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

- El campo IHL (*Internet Header Length*) o longitud de la cabecera de interred, indica la longitud de la cabecera en palabras de 32 bits. El tamaño mínimo admitido es de 5 palabras, llegando hasta la dirección destino. Este campo también está compuesto por 4 bits. El campo tipo de servicio, es un campo de 8 bits. Este campo indica la calidad del servicio deseado. Estos parámetros se utilizan para guiar la selección de los parámetros del actual servicio o tecnología que se está utilizando cuando se va a transmitir el datagrama a través de una red en particular. Es decir el efecto de los valores de estos campos depende de la tecnología de la red utilizada.

- El TOS (*Type of service*) se utiliza para manejar cierta prioridad en el tráfico que se está transmitiendo, pues por ejemplo para la transmisión de voz digital es más importante la velocidad y no la entrega precisa, caso contrario sucede con la transferencia de archivos en donde es más importante una entrega sin errores que una entrega rápida. Este campo es uno de los campos que ha cambiado levemente su significado en el transcurrir de los

años. En sus inicios este campo usaba 3 bits para un sub campo denominado precedencia ó prioridad, además usaba otros 3 bits que se les denominaba banderas, que eran D (*Delay* o retardo), T (*Troughput* o velocidad real de transporte) y R (*Reliability* o confiabilidad), los últimos dos bits no se utilizaban y aún hoy en día se tienen reservados para un futuro uso, es por ello que se decía que este campo constaba de 6 bits. ***(Ver Imagen N° 21)***

Imagen N° 21: Formato de Campo TOS



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

- El campo longitud, es un campo compuesto por 16 bits, que nos indica la longitud total del datagrama, medido en octetos (8 bits) o bytes, que incluye la cabecera y los datos. Este campo es necesario pues indica donde termina un datagrama y con ello se puede determinar cuándo comienza otro datagrama. Dado que está compuesto de 16 bits, la longitud máxima es de 216 - 1= 65,535 bytes. Esta longitud ya no es tolerable para redes GigabitEthernet, las cuales requieren datagramas más grandes. Es normado que las estaciones envíen únicamente datagramas de longitud de por lo menos 576 bytes.

- El campo identificación es un campo de 16 bits, el cual es necesario para que la estación determine a qué datagrama pertenece un fragmento recién recibido. Esta identificación es asignada por el emisor para ayudar en el

ensamblaje de los fragmentos del datagrama, existe un único identificador para todos los fragmentos que corresponden a un mismo datagrama.

- El siguiente es el campo de Flags o banderas, el cual está compuesto por 3 bits que también se les denomina indicadores de control. El bit más significativo o bit 0, está reservado y su valor debe ser 0. El bit 1 ó bit DF (*Don´t fragment* o no fragmentar), puede tomar los valor de 0 el cual indica a los enrutadores que el datagrama puede fragmentarse y el valor de 1 cuando no se puede fragmentar. El bit menos significativo (bit 2) o bit MF (*More Fragments* o más fragmentos), éste es un indicador que tienen todos los fragmentos excepto el último que conforma el datagrama, pues indica cuando han llegado todos los fragmentos al destino.

- El campo Fragment offset o desplazamiento de fragmento, es un campo de 13 bits, el cual indica en qué parte del datagrama actual va un fragmento en específico. Todos los fragmentos exceptuando el último deben tener un múltiplo de 8 bytes, que es la unidad de fragmentos elemental. El máximo de fragmentos por datagrama es de 213 = 8192.

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

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

- El campo checksum header o suma de verificación de cabecera, es un campo compuesto de 16 bits, el cual su función es hacer una suma de verificación para la detección de errores generados por palabras de memoria

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

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

- El último campo en este datagrama de IP versión 4, es el campo de opciones, este campo como su nombre lo indica puede o no utilizarse. Este campo cuando se usa en IPv4 su función muchas veces es para hacer experimentos, probar nuevas ideas y para evitar la asignación de bits de encabezado a información pocas veces necesaria. Este campo es de longitud variable. Cada opción comienza con un código de 1 octeto. Algunas opciones van seguidas de un campo de longitud y luego de uno o más octetos de datos. Este campo es utilizado para completar múltiplos de 32 bits o sea 4 octetos. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009] ***(Ver Tabla N° 01)***

Tabla N° 01 Tipos de opciones del datagrama

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

		dirección IP.
8	Identificador de línea	Lleva la identificación de la línea.
9	Enrutamiento estricto desde el origen	Indica la ruta completa a seguir.

Algunas de estas opciones son bien importantes como la de seguridad, la de enrutamiento estricto desde el origen, la de enrutamiento libre desde el origen, la de registrar ruta y la opción marca de tiempo. La opción seguridad se usa para especificar que el datagrama se encamine por una cierta ruta, la cual se considera una ruta segura, esto podría servirle a la milicia, si ellos no quisieran que su información pase por cierto país. **(Ver Imagen N° 21)**

Imagen N° 21: Formato de la opción seguridad en IPv4

- El campo S, es un campo de 16 bits que especifica uno de los 16 niveles de seguridad, ocho de los cuales están reservados para futuros usos.

- El campo C, es un campo de 16 bits, es un campo que si todos sus bits tienen valor igual a cero, entonces la información no está compartida, otros valores para este campo pueden ser obtenidos de la Agencia Inteligente de Defensa.

- El campo H, es un campo de 16 bits que se encarga de las restricciones. Dichas restricciones están definidas en el DIAM 65-19 (Manual de la agencia inteligente de defensa).

- El campo TCC o código de control de transmisión (*Transmision Control Code*), es un campo de 24 bits que define comunidades de interés controladas entre suscriptores.

La opción de enrutamiento estricto desde el origen, brinda la ruta completa desde el origen hasta el destino. Es necesario que el datagrama siga dicha ruta exacta. Esto es utilizado cuando en un enrutador se pierde la tabla de

enrutamiento y es necesario enviar datagramas de emergencia con la ruta especificada. Esto quiere decir que el paquete debe seguir exactamente cada uno de los saltos que se especifican en dicha ruta, no puede tomar una ruta alterna, aunque dicha ruta alterna sea mejor. La opción de enrutamiento libre desde el origen, requiere que el datagrama pase por los enrutadores indicados en la lista, y en el orden especificado, pero puede pasar por otros enrutadores en dicho trayecto. La opción de registrar ruta, indica a los enrutadores que registren su dirección IP al campo de opción. Con esto los administradores de las redes pueden determinar fallas en los algoritmos de enrutamiento.

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

3.2. Direccionamiento de IPv4

El protocolo IP es un protocolo enrutado el cual ofrece direccionamiento, fragmentación y reensamblaje de datagramas y entrega de datagramas a través de la interred. Una dirección IP en versión 4 está compuesto por 4 campos de 8 bits y cada campo es separado por un punto “.”. El direccionamiento IP o direccionamiento de capa de internet es necesario para poder identificar a una interfaz de un dispositivo con una única dirección como miembro de una red en específico, pues la identificación de un nodo en una interred requiere el uso de la red a la que pertenece y la identificación del nodo en dicha red. La dirección IP no es igual que la dirección MAC, pues la dirección IP está en la capa 3 del modelo OSI y la dirección MAC en la capa 2. La dirección MAC es una dirección física fija que es asignada por el fabricante de la interfaz, mientras que la dirección IP es una dirección lógica que puede variar para cada interfaz. La dirección IP es la dirección utilizada por los protocolos de capas superiores y ésta puede soportar cambios de hardware, pues si se cambiara la tarjeta adaptadora de red de un host, su dirección IP puede configurarse para que sea la misma y no varíe.

3.2.1. Formato de una dirección IPv4

Una dirección IP en versión 4 es un conjunto de unos y ceros cuya longitud es de 32 bits, lo cual da (2a la 32) = 4,294,967,296 direcciones IP posibles. Como

se mencionó anteriormente cada octeto está separado por un punto, el primer octeto es el de la izquierda y el cuarto octeto es el de la derecha. El formato que se maneja es en base decimal para que su uso sea más sencillo y comprensible, esto se muestra a continuación:

- Dirección IP en base 2 (Formato binario): 10101100.00010000.00000011.01010101
- Dirección IP en base 10 (Formato decimal): 172.16.3.85

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

Las direcciones IP constan de dos campos, los cuales son, el campo de identificador de red o netid, y el campo identificador de host o hostid. El campo identificador de red es el encargado de identificar a que red pertenece la estación, y el campo identificador de host es el identificador asignado único para cada interfaz, servidor, encaminador o cualquier otra estación en específico [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

3.2.2. Clases de Direccionamiento en IPv4.

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

Imagen N° 22: Clases de direcciones IPv4

En las direcciones clase A, el primer octeto es identificador de red y los tres restantes son de host, estas direcciones comienzan con un valor igual a cero en el bit más significativo. El rango de esta clase es de 0 a 127 (00000000 – 01111111)2, el número de redes posibles es 27 = 128 – 2 = 126 redes. Se le 81 resta 2 pues uno de estos valores es un valor reservado y el otro es una restricción. La restricción es debido a que la dirección 0.0.0.0 fue definida originalmente como dirección de broadcast. El valor reservado es utilizado para pruebas y a esta red se le conoce como red Loopback (127.0.0.0) o bucle cerrado, esta red se utiliza para que un host, encaminador o cualquier otro dispositivo que tenga una interfaz pueda enviar paquetes hacia ellos mismos y pueda comprobar si está bien la interfaz o no. El número de host o estaciones por red es de 224 = 16,777,216 – 2 = 16,777,214. Se le resta dos, pues en cada red o subred, se debe tener una dirección que la identifique, además debe tener una dirección de multidifusión o como más comúnmente se le conoce dirección de broadcast.

En las direcciones clase B, el primer y segundo octeto son identificadores de red y el tercer y cuarto octetos son los identificadores de host. Las direcciones clase B comienzan por los bits 1 y 0 en su primer octeto, el rango de esta red es de 128 a 191 (10000000 – 10111111)2. El número de redes posibles es igual a 2(6+8) = 214 = 16,384 – 2= 16,382 redes posibles, se restan dos debido a que existen dos redes que están reservadas (128.0.0.0 y 191.255.0.0). El número de host por red es 216 = 65,536 – 2= 65,534 estaciones.

En las direcciones clase C, el primer, segundo y tercer octeto son identificadores de red y sólo el último octeto es identificador de host. Estas direcciones comienzan con sus primeros tres bits del primer octeto con valores binarios de 110, es por ello que el rango de esta clase es de 192 a 223 (11000000 – 11011111)2. El número de redes posibles es igual a 2(5+8+8) = 221 = 2,097,152 – 2= 2,097,150, se le restan dos debido a que en esta clase también existen dos redes reservadas (192.0.0.0 y 223.255.255.0) y el número de hosts por cada red es de 28 = 256-2 =254. 82

La clase D, es una clase creada para permitir multicast en una dirección IP. Como se mencionó una dirección multicast es una dirección que permite direccionar paquetes enviados a dicha IP hacia grupos predefinidos de

direcciones IP, esto quiere decir que un solo host puede trasmitir los mismos paquetes hacia múltiples receptores de forma simultánea. Los primeros cuatro bits del primer octeto de esta clase deben ser 1110, es por ello que el rango de esta clase es de 224 a 239 (11100000 – 11101111)2. En esta clase el número de bits del identificador de host es de 28 bits. La última clase es la clase E, la cual es una clase reservada por la Fuerzas de Tareas de Ingeniería de Internet (IETF), para propósitos de investigación. Los primeros cuatro bits de una dirección perteneciente a esta clase deben ser 1111, es por ello que el rango de esta clase es de 240 a 255 (11110000 – 11111111)2. El número de bits de identificador de host es de 28 bits al igual que la clase D. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

3.2.3. Direcciones IP Privadas y Públicas

Para que una red sea administrable y que cada dispositivo se pueda direccionar, es necesario que se asigne una única IP por cada dispositivo y esa dirección no sea repetida en toda la red. Debido a que Internet es el conjunto de varias redes, no se puede repetir una IP para dos o más estaciones que estén conectadas en Internet aunque pertenezcan a diferente red. Es por ello que la IEEE decidió definir dos tipos de direcciones IP, la primera son las direcciones privadas y la segunda son las direcciones públicas. [Tanenbaum and Wetherall, Computer Networks, 2011]

3.2.3.1. Las Direcciones Públicas

Son aquellas que se utilizan para direccionar estaciones que se conectan a Internet. Las direcciones públicas son exclusivas, pues estas son globales y están estandarizadas. En un inicio estas direcciones eran asignadas por la InterNIC (Centro de información de la red Internet), pero después ésta desapareció y este trabajo ahora lo ejecuta la IANA (Agencia de asignación de números de Internet), esto es para que la asignación de IP públicas sea controlada y regulada cuidadosamente para garantizar que no se genere una asignación de una dirección repetida.

3.2.3.2. Las Direcciones Privadas

Son aquellas que se utilizan para direccionar estaciones en una LAN privada, la cual no tiene salida al Internet, o si la tiene es a través de un NAT (*Network Address Translation* o traducción de dirección de una red). Este tipo de direcciones sí se puede repetir en varias redes siempre y cuando dichas redes no tengan comunicación entre sí. Esta fue una solución inmediata al problema de la escasez de IP´s públicas, pues dentro de una red la cual no tenga salida a Internet, no es necesario asignarles IP´s públicas. Una red privada podría utilizar cualquier dirección IP definidas en las distintas clases que se mencionaron anteriormente, pero es recomendable que se escoja dicha dirección de acuerdo al número de estaciones que van a haber por red, al número de redes que se quiere formar y si tendrá salida a Internet o no. Es por ello que en el RFC 1918 se definieron tres bloques de direcciones IP privadas dependiendo del tamaño de la red (clase A, B o C). Estas direcciones no se encaminan hacia el backbone de Internet, su uso es exclusivo para redes privadas y tampoco se puede utilizar para direccionar estaciones en Internet. Las estaciones en las redes pueden ser divididas en tres categorías.

En la primera categoría se encuentran todas las estaciones que no requieren el acceso a otra red ni a Internet, en esta categoría las estaciones pueden utilizar direcciones IP iguales entre diferentes redes.

En la segunda categoría se encuentran las estaciones que necesitan acceder a aplicaciones como correo electrónico, un servidor FTP, Telnet, esto quiere decir que una red se pueda comunicar con otras redes, pero no necesita salir a Internet, en esta categoría las estaciones pueden utilizar direcciones IP que sean repetidas entre las diferentes redes (si y sólo si no tiene comunicación con una estación en diferente red pero con la misma IP) y que solamente necesiten conectarse a un servidor como FTP y no establecer comunicación entre ellas. En la última categoría o categoría 3, se encuentran las estaciones que necesitan salir a Internet, en este tipo de categoría es necesario que cada estación tenga una única dirección IP, o pueden tener repetidas IP privadas, pero al momento de anunciarse en internet tienen que tener una IP pública única.

Las direcciones IP privadas son las que están dentro de la categoría 1 y las direcciones IP públicas son las que están dentro de la categoría 3.

Las direcciones privadas reservadas por la IANA se muestran en la Tabla N° 02. [Tanenbaum and Wetherall, Computer Networks, 2011]

Tabla N° 02: Tabla de direcciones privadas

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

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

3.2.4. División de Redes en Subredes

Se utiliza la división de una red en subredes para administrar las direcciones IP que se tienen en una red en particular, dado que con dicha división se logra segmentar toda una red grande en subredes más pequeñas para poder tener redes de un número reducido de hosts en una misma red. El precio que hay que pagar por una mejor administración de direcciones IP es el de perder dos direcciones IP por cada nueva subred. La división de redes es utilizada también debido a las pocas direcciones IP públicas que existen. Para poder llevar a cabo dichas subredes, es necesaria una máscara de subred, la cual es una máscara no por defecto utilizada para poder tomar algunos bits del campo de host y convertirlos en bits de subred. Se menciona una máscara no por defecto, pues para las tres principales clases de redes. [Tanenbaum and Wetherall, Computer Networks, 2011] **(Ver Tabla N° 03)**

Tabla N° 03: Tabla Máscaras por defecto

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

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

3.3. Enrutamiento Y Transporte

El enrutamiento es el proceso de mover paquetes o datagramas de una red a otra red usando para ello los enrutadores los cuales trabajan en la capa 3 del modelo OSI. Es importante recalcar nuevamente la diferencia entre un protocolo enrutado y un protocolo de enrutamiento. En nuestro enfoque el protocolo enrutado es IP y algunos ejemplos de protocolos de enrutamiento son OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*) y EIGRP (*Enhanced Interior Gateway Routing Protocol*).

Un protocolo de enrutamiento es utilizado por los enrutadores para que dinámicamente puedan hallar todas las redes en la interred y asegurar que los demás enrutadores posean esta tabla de enrutamiento, así de esta manera pueda determinarse el camino que debe seguir un paquete a través de toda la interred para poder llegar a su destino. Una vez que se conocen todas las redes, un protocolo enrutado es usado para enviar los paquetes del usuario.

Un enrutador también puede conocer las rutas hacia las diferentes redes estáticamente. Esto quiere decir que alguna persona definió por medio de comandos propios del enrutador, cuál debería de ser la ruta que el paquete debe de tomar cuando se dirige a una red destino.
Este tipo de enrutamiento tiene sus ventajas y desventajas. Una ventaja podría ser que consume menos ancho de banda para conocer todas las rutas, y una desventaja podría ser que cuando se está trabajando con redes grandes, se vuelve bastante complejo poder configurar todas las rutas.

Otra desventaja podría ser que si se cae un enlace, el enrutador no puede saber qué otro camino tomar, a menos que se haya configurado. Para poder enrutar paquetes un enrutador debe de saber cómo mínimo la dirección IP destino, los vecinos de quien puede aprender las rutas hacia las distintas redes, las posibles rutas a todas las redes, la mejor ruta a cada red y como mantener y verificar la información de enrutamiento. [Tanenbaum and Wetherall, Computer Networks, 2011]

3.3.1. Protocolos de enrutamiento dinámico

Un protocolo de enrutamiento es el esquema de comunicación entre routers. En un protocolo de enrutamiento dinámico si la red está directamente conectada al enrutador, entonces el enrutador ya conoce la red, pero si no está directamente conectada, entonces debe de hacer su tabla de enrutamiento. Una vez formada la tabla de enrutamiento y si ocurre algún cambio dentro de la red, el enrutador informa a todos sus vecinos de los cambios hasta que la red converja o sea hasta que todos los enrutadores de la red tengan la misma tabla de enrutamiento. [Peterson and Davie, 2011].

Los protocolos de enrutamiento aprenden todas las rutas disponibles, incluyen las mejores rutas en la tabla de enrutamiento y descartan las que no son válidas. En este punto, toma bastante relevancia el AS (*Autonomous System*) o sistema autónomo, que es un conjunto de redes que están bajo una administración común, el cual cuenta con sus propias reglas y políticas, y que comparten una estrategia de enrutamiento común hacia el exterior.
Estos AS son asignados por la ARIN y es un número de 16 bits.

3.3.1.1. IGP´s

Los IGP (*Interior Gateway Protocol*) son protocolos de enrutamiento interior, que se les denomina interior porque son los que se pueden utilizar dentro de un AS. Los IGP´s están clasificados en base a cómo funcionan sus algoritmos, pues existen algoritmos que se basan en la distancia los cuales se les denominan vector-distancias, también están los protocolos basados en el estado del enlace.

Este tipo de protocolo envía periódicamente la tabla de enrutamiento completa a los routers vecinos, con lo cual pueden mantener la topología de la red, en base a lo que cada router va observando en sus vecindades. Las tablas de enrutamiento incluyen información acerca del costo total de la ruta, la cual está definida por su métrica y la dirección IP del primer router en la ruta hacia cada una de las redes.

Protocolo RIP (*Routing Information Protocol*) o protocolo de información de enrutamiento y el IGRP (*Interior Gateway Routing Protocol*) o protocolo de enrutamiento de salida interior. RIP es un protocolo que utiliza como métrica el número de saltos y es un protocolo bajo estándares públicos. El IGRP es un protocolo propietario de la marca Cisco, y que su métrica está compuesta por la combinación de variables como retardo, ancho de banda, confiabilidad y carga.

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

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

el otro protocolo de enrutamiento dinámico de estado de enlace, el cual hace uso también de SPF.
Es un protocolo de gran escalabilidad y de rápida convergencia al igual que OSPF. IS-IS integrado puede trabajar con protocolos OSI, así como con protocolos IP.
Si se trabaja en el modo OSI los routers IS-IS no deben de configurarse en capa 2 sólo en capa 1, pero si se trabaja en áreas IP puras, los routers se pueden configurar capa 2. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

3.3.1.2. EGP´s

Los EGP (*Exterior Gateway Protocols*) o también denominados protocolos de enrutamiento externo, son los encargados de proveer el enrutamiento entre sistemas autónomos. Este tipo de protocolo es el que utiliza un ISP (*Internet Service Provider*), y es el que se utiliza en los routers del corazón de internet.

Un EGP necesita de un conjunto de información antes de comenzar su operación, una lista de routers vecinos, una lista de redes a ser publicadas como de acceso directo y el número de sistema autónomo del router local. El BGP (*Border Gateway Protocol*), es un protocolo de enrutamiento externo robusto que se utiliza entre sistemas autónomos, debido a esto se convirtió en el protocolo más utilizado en toda Internet. Para lograr la escalabilidad a este nivel, BGP utiliza varios parámetros a los cuales se les denomina atributos, con esto logra definir las políticas de enrutamiento y mantener un ambiente estable de enrutamiento. Además para reducir el tamaño de las tablas de enrutamiento, BGP hace uso de CIDR (*Classless Interdomain Routing*). En las actualizaciones de las tablas de enrutamiento que se realizan entre vecinos, primero se debe de establecer una conexión TCP entre dichos vecinos y así únicamente cuando se produce un cambio en alguna ruta, estos cambios son anunciados a los vecinos. Las rutas aprendidas vía BGP traen asociadas propiedades, las cuales son utilizadas para determinar la mejor ruta a un destino, cuando existen múltiples rutas hacia un mismo destino. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

3.4. Seguridad en IPv4

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

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

El protocolo IP en sus inicios no contaba con una seguridad generalizada en la capa IP. Con el transcurrir del tiempo la seguridad se fue añadiendo en las capas de aplicación, tales como SSL (*Secure Socket Layer*) para aplicaciones WEB. En la actualidad se cuenta con una gran variedad de opciones de seguridad que inclusive se repiten en los distintos protocolos de aplicación, creando todo un grupo de nuevos problemas, tales como múltiples, diferentes e incompatibles funciones de gestión de llaves.
Una de las primeras soluciones y de mucha importancia para la seguridad en las redes es el cifrado, el cual es una transformación carácter por carácter o bit por bit, sin importar la estructura lingüística del mensaje. Otra solución fue la utilización de firewalls y listas de control de acceso. Pero aún con estas soluciones con ciertas limitaciones, se necesita una opción más completa, y es por ello que la IETF decidió trabajar en un protocolo de seguridad que trabajara en la capa IP, por lo cual nace IPsec el cual está definido en el RFC 2401; sin embargo, el desarrollo de IPsec en la actual versión de IP (IPv4) ha presentado dificultad en la protección de paquetes IP cuando se utiliza NAT, es por ello que el estudio de IPsec se verá cuando analizemos IPv6, para poder analizar los beneficios que se obtiene con IPv6. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

3.4.1. Criptografía y sus Algoritmos

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

3.4.1.1. El Cifrado Convencional o Simétrico

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

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

3.4.1.2. Algoritmo de descifrado:

Los dos algoritmos de cifrado convencionales de bloque más importantes son, el DES (*Data Encryption Standard*) y el TDEA (*Triple Data Encryption Algorithm*).
El cifrado de clave pública, fue el primer avance revolucionario en el cifrado debido a que éste estaba basado en funciones matemáticas y no en substituciones y transformaciones como el cifrado convencional. Este tipo de cifrado contiene seis ingredientes:

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

En IPv4, se utiliza mucho la encriptación ya sea con el cifrado convencional o con el asimétrico, debido a la falta de seguridad del protocolo IP. Dicha seguridad es mejorada en su nueva versión IPv6, como se verá más adelante. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

3.4.2. Protección de una Red Utilizando un Contra Fuegos

Otra solución que se dio para mejorar la seguridad en redes IP utilizando versión 4, fue la introducción de un contra-fuegos o firewall. Un firewall es una estructura arquitectónica que existe entre el usuario y el mundo exterior para proteger la red de intrusos que vienen de Internet.
Un firewall tiene dos componentes: dos enrutadores que realizan filtrado de paquetes y una puerta de enlace de aplicación. El primer enrutador filtra los paquetes de entrada y si cumplen con el criterio de filtrado entonces los reenvía de manera normal, pero si no cumple entonces desecha dichos paquetes, igual trabajo realiza el segundo enrutador a excepción que este trabaja con los paquetes de salida de la red. El criterio del filtrado puede ser un bloque de direcciones IP que están autorizados para entrar, o posiblemente que algunos puertos o sockets de aplicación pueden estar autorizados y otros no. La otra parte del firewall es la puerta de enlace de aplicación, la cual está dedicada a examinar cada mensaje que entra o sale pero a nivel de aplicación, por ejemplo configurar una puerta de enlace de correo y con ello examinar los mensajes que entran y salen de la red para bloquear y aceptar ciertos tipos de mensajes.

En los enrutadores firewall de entrada y salida, se deben de utilizar ACL (*Access Control List*) o listas de control de acceso, con ello se logra conseguir tener el control del tráfico entrante y saliente de alguna parte específica de la red. Las ACL son muy útiles pues se pueden crear ACL´s en base a la dirección IP, el tipo de protocolo enrutado y el número de puerto, por cada interfaz del enrutador, tanto para el tráfico entrante como para el tráfico saliente. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

3.5. Limitación a Corto Plazo de IPV4

La necesidad de la actualización del protocolo IP, surgió desde los años 1980s, cuando se pudo predecir en base al continuo crecimiento de Internet que se estaba dando en esa época. En IPv4 se cuenta con la capacidad de poder direccionar 232 = 4,294,967,296 hosts, con lo cual uno podría pensar que es suficiente para poder acomodar fácilmente cientos de millones de hosts hacia Internet. Sin embargo, esto funcionaría si las direcciones IP se distribuyeran de forma secuencial, lo cual no es posible debido a su forma jerárquica de direccionamiento. Como se mencionó una dirección IP consta de dos partes, la primera es el identificador de la red y la segunda es el host al cual identifica.

Esta forma jerárquica de direccionamiento fue definida de esa manera para poder fácilmente encaminar los paquetes de un host a otro, pues en el enrutamiento primero se encamina el paquete hacia la red a la que le corresponde, según la IP, y luego ya que se ha llegado a la red, se dirige el paquete al host que le pertenece, según también la IP. Con el escaseo de direcciones IP, la IANA empezó a asignar las direcciones IP de una manera más restrictiva, y para organizaciones grandes que solicitaban redes clase B, se les otorgaba y se les sigue otorgando, siempre y cuando estén bien justificadas, y sólo se les asigna quizá una subred de una clase B. Las redes clases C son las que más comúnmente son asignadas, pero éstas tienen la limitación que pueden funcionar para redes pequeñas. Esta limitación de asignaciones de IP´s públicas es una de las limitaciones más notables y críticas de IPv4, pero no es la única. Una necesidad que surge con la evolución de las computadoras es la movilidad, pues inicialmente las computadoras eran grandes cuartos de equipos, y hoy día existen una gran variedad de computadoras portátiles las cuales necesitan poder conectarse en Internet. En IPv4 un avance en la movilidad es el DHCP, pero con este protocolo aún se continúa dependiendo de un solo punto de conexión a la red, pues el host se mueve de dicho punto y desea conectarse a la red en un punto que no es un punto de conexión de su ISP, entonces debe volver a realizar una nueva conexión con los datos de este nuevo ISP (Gateway, máscara de subred y DNS).

Debido al problema de que no existen muchas direcciones IP públicas, se decidió trabajar con subredes de las distintas clases de redes existentes, y con

ello optimizar el espacio de direccionamiento. Además con las subredes se podía adaptar el esquema de direccionamiento a las necesidades de las redes de cada organización. Lamentablemente organizaciones que necesitaban una clase B y lo solicitaban tenían que esperar mucho tiempo para que se las asignaran o en el peor y más común de los casos no se las asignaban y lo que les podían asignar eran varias clases C, pero esto iba haciendo mucho más largas las listas de enrutamiento. La limitante de que las tablas de enrutamiento se iban haciendo cada vez más largas, fue solucionado con una herramienta llamada CIDR. Las listas de enrutamiento habían estado creciendo enormemente, mientras más y más redes se agregaban, y esto se traducía en mucha más latencia para Internet, o lo que es lo mismo mucho más tiempo a que un paquete pudiera llegar a su destino, pues cuando el paquete llegaba a un router, se tenía que buscar en toda la lista de enrutamiento cuál debía ser el siguiente salto para poder llegar a la red destino, y con el crecimiento que venía teniendo y sigue teniendo Internet las listas eran enormes. Con CIDR se logró solventar dicho problema, pues como es un enrutamiento sin clase, lo que significa que con esto se le indica al router que ignore la clase a la que pertenece una subred o lo que es lo mismo que se haga una superred de las diferentes subredes, logrando así que la tabla de enrutamiento sea más pequeña, lo que se traduce como una mejora en el desempeño del enrutamiento y una menor latencia en todo Internet. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009].

CAPÍTULO IV

ANÁLISIS DEL PROTOCOLO IPv6

IV. ANÁLISIS DEL PROTOCOLO IPv6

En el actual capítulo abordaremos a detalle el protocolo IPv6, así como también se verá la distribución actual de recursos de Internet, quién es la mayor autoridad.

4.1. Historia del Protocolo IPv6.

La historia de Ipv6 se inició en el año 1990, cuando se reveló que las direcciones IPv4disponibles estaban disminuyendo aceleradamente.
Según estudios realizados por profesionales que indicaban que las IPv4 se agotarían alrededor del 2005. Dichos estudios fueron muy cuestionados por toda la comunidad de Internet, y es de ahí que iniciaron la búsqueda de posibles soluciones. Para ese entonces se plantearon dos soluciones:[Dunmore, 2005]

1. Mínimo: Salvaguardar el protocoloIPv4, es decir, mantenerlo intacto, sólo se debe aumentarla longitud de la dirección. Esto es muy sencillo, lo que ocurriría es tener menos suplicio en la fase de despliegue.
2. Máximo: Desplegar completamente la nueva versión del protocolo IPv6, cuyo enfoque permitiría incorporar nuevas características y mejoras en IPv4.

Debido a que no existía tanta urgencia en plantear una solución rápida, el desarrollo de un nuevo protocolo fue elegido, es decir, que el nombre original fue IPng (Próxima generación IP, IP Next Generation) mismo que fue desplazado por IPv6, siendo este el nombre definitivo, llevados de la mano por Steven Deering y Robert Hinden.

El primer conjunto de protocolos RFCs que rigen al IPv6, fue presentado finalizando el año 1995, dicho protocolo se lo denomino RFC 1883: Protocolo de Internet versión 6 (IPv6). Una vez que se tenía disponible el RFC 1883 las implementaciones fueron esperadas con entusiasmo, pero nunca ocurrieron. Para ese entonces (década del año 1990) el auge significativo de Internet en empresas causo incertidumbre entre ellas, donde tenían que resolver un complicado problema de negocio, invertir en IPv6 que traería algunos beneficios a futuro, o invertir en el despliegue de IPv4, ya que cualquiera de los dos protocolos (IPv6 e IPv4) les representarían ganancias. Finalmente la mayoría de las empresas decidieron escoger el retorno rápido y fácil de las inversiones y desarrollaron productos basados en IPv4.

Surgieron otros métodos para mantener el espacio de direcciones, el más importante es el enrutamiento sin clase entre dominios (CIDR, Classless Inter-Domain Routing), como consecuencia, los sitios recién conectados obtuvieron significativamente menos direcciones que en años anteriores. El uso del CIDR retraso la implementación de IPv6 ante los ojos de muchas personas, pero no en todos.

Aquellos sitios nuevos o en expansión desarrollaron métodos para limitar este recurso, uno de estos enfoques ha sido la traducción de dirección de red (NAT, Network Address Translation) que permitió utilizar a las redes de computadoras un número cualquiera de direcciones privadas, y para luego convertirlas en públicas cuando los paquetes dejaran el sitio y viceversa. NAT utiliza el mecanismo de compartir direcciones públicas a través de hosts, así como otros mecanismos tales como PPP (Point to Point Protocol) y DHCP (Dynamic Host Configuration Protocol) proporcionan un medio para que hosts alquilen direcciones por un cierto período de tiempo. [Blanchet, Marc. Migrating to IPv6, 2006]

4.2. Protocolo de IPv6

El Protocolo de Internet versión 6 (IPv6) ha sido definido por el RFC-2460, cuyo diseño ha sido para sustituir alIPv4 (RFC 791), en la actualidad se están incorporando en la gran mayoría de dispositivos electrónicos que acceden a Internet tales como: placas de red, switches, routers y todo dispositivo de conectividad. Steve Deering de Xerox PARC y Craig Mudge fueron los que crearon y diseñaron el protocolo de internet IPv6 destinado a sustituir a IPv4, cuyo límite en el número de direcciones de red admisibles está empezando a restringir e impedir el crecimiento de Internet y su uso en países de gran densidad de población como: China, India, y otros países Asiáticos, en Ecuador hay aproximadamente 7 millones de usuarios a junio 2012.

Dicha versión (IPv6) mejorará el servicio globalmente; por ejemplo, proporcionará a futuras celdas telefónicas y dispositivos móviles sus direcciones propias y permanentes, esto no sería poca cosa. A inicios del 2010 se tenía al menos 10% de IP's disponibles. Es por esto que la IANA (Agencia Internacional de Asignación de Números de Internet, por sus siglas en inglés) entregó en febrero 2011 el último bloque de direcciones disponibles (33 millones) a la

organización encargada de asignar IP's en Asia, un mercado que está en auge y no tardará en consumirlas todas, por lo que hemos mencionado anteriormente, su gran crecimiento en población. Esta nueva revisión del protocolo IP se numerará con la versión 6 y no versión 5 para evitar confusiones, ya que anteriormente se hicieron pruebas añadiendo extensiones a la versión 4. Dichas extensiones experimentales no terminaron de formalizarse con una nueva versión del protocolo, por esto fue preferible evitar posibles conflictos de numeración, razón por la cual el número de versión es 6. Bajo estas circunstancias, IPv6 conocido también como IPng (IP de próxima generación) ofrece mayor flexibilidad y eficacia para dar soluciones a una amplia gama de nuevos problemas. Los principales objetivos que sigue IPv6 son: [Blanchet, Marc. Migrating to IPv6, 2006]:

a) Admitir miles de millones de equipos, superando las limitaciones de espacio para las direcciones IPv4 actuales;

b) Reducir el tamaño de las tablas de enrutamiento;

c) Simplificar el protocolo para permitir que los routers enruten datagramas de manera más rápida;

d) Brindar mejor seguridad (autenticación y confidencialidad) que la proporcionada por el protocolo IP actual;

e) Prestar más atención al tipo de servicio y, particularmente, a los servicios asociados con el tráfico en tiempo real;

f) Facilitar la difusión a destinos múltiples, permitiendo especificar el tamaño;

g) Permitir la movilidad de un equipo sin cambiar su dirección;

h) Permitir el futuro desarrollo del protocolo;

i) Posibilitar la coexistencia pacífica del protocolo antiguo con el nuevo.

4.3. Características de IPv6.

El diseño de IPv6 por parte de la IETF es una nueva versión del protocolo de Internet que fue diseñado como un paso evolucionario más que como un paso revolucionario de IPv4. Muchas de las buenas funcionalidades de IPv4 se

mantuvieron y otras que no eran tan buenas fueron removidas, así como otras funcionalidades nuevas que fueron agregadas. A continuación se listan y detallan de manera breve algunas de las características de IPv6, que serán tratadas a mayor profundidad más adelante: [Blanchet, Marc. Migrating to IPv6, 2006]

- Direcciones más largas, pasando de una dirección de 32 bits a una dirección de 128 bits, lo cual permite direccionar 340,282,366,920,938,463,374,607,431,768,211,456 nodos, eliminando así la necesidad de NAT.

- Más niveles jerárquicos de direccionamiento, lo cual provee una eficiente, jerárquica, y sumarizada infraestructura de enrutamiento, o sea una mejor agregación de rutas.

- Arquitectura de direcciones simple y fija, lo cual permite una fácil planificación y con ello se reduce el costo de manejo de las redes. Ahora en IPv6 las máscaras de subred son fijas y proveen una virtual cantidad ilimitada de nodos en un enlace.

- Direcciones privadas, éstas están compuestas por bits específicos en la dirección para las redes que no van a estar conectadas a Internet. Estas son diferentes a las redes privadas IPv4 del RFC1918, pues en IPv6 estas direcciones permanecen únicamente asignadas a una red o a un nodo, lo cual hace que la conectividad entre redes privadas sea más fácil.

- Nodos autoconfigurables, esto está basado en los anuncios que envían los encaminadores, en la cual los nodos insertan su dirección MAC en la parte de la dirección de host en IPv6.

- No hay conflictos de direcciones en enlaces, esto es debido a que en la parte de host de IPv6 se incrusta una única dirección MAC que garantiza que no habrá otra dirección igual.

- Alcance del direccionamiento Multicast, que ahora en IPv6 se tiene un alcance del enlace que está dentro de la dirección Multicast, mientras que en IPv4 se tenía que confiar en el TTL.

- Una cabecera más simple y eficiente, pues ahora se cuenta con menos números de campos, no hay checksum, lo cual hace que los encaminadores procesen los paquetes más rápido y más eficientemente.

- IPSec obligatorio, en IPv6 se dice que la seguridad aumenta, debido que IPsec que en IPv4 era opcional para mejorar la seguridad, en IPv6 se vuelve obligatorio.

- Transición simple y flexible, este fue un requerimiento de que el nuevo protocolo fuera simple y flexible en su transición y con un bajo costo.

- Mejor soporte para QoS (*Quality of Service*), esto es debido a que hay nuevos campos en la cabecera IPv6 que definen cómo el tráfico se manejará e identificará en tiempo real, esto inclusive aunque el campo de carga útil esté encriptado. Esto es debido al campo de IPv6 que se llama "Flow Label" o Etiquetado de flujo.

El protocolo de internet versión (IPv6) conserva muchas de las características que hicieron exitoso a IPv4, dentro de las cuales se puede destacar que opera sin conexiones, es decir, que cada datagrama tiene una dirección de destino y su enrutamiento es independiente. También resaltamos que como IPv4, la cabecera de cada datagrama tiene una cantidad máxima de saltos que deben de hacerse antes de descartarlo. Sin embargo existen otras características que además de ser conservadas, y que IPv6 también se encarga de mejorarlas. (Pinillos, 2003)
Existen características muy interesantes que IPv6 trae consigo, ya que resuelven muchos de los problemas de la versión 4. Las características más importantes de IPv6 se describen a continuación: [Blanchet, Marc. Migrating to IPv6, 2006]

a. Direccionamiento. (Pinillos, 2003) El campo para direccionar o identificar dispositivos es de 128 bits (2128), este campo es lo suficientemente grande para manejar el crecimiento continuo de Internet mundial durante muchas décadas. El número de direcciones IP que ofrece IPv6 es alrededor de 340 sextillones.

b. Rendimiento. (Pinillos, 2003) Actualmente, las redes LAN y WAN están progresando respecto a la velocidad de transmisión, pudiendo utilizar

velocidades de ciento de Megabits por segundo con la tendencia de llegar a varios Gbps (Gigabits por segundo). Esto se debe a que la tecnología mejora día a día y la existencia de la necesidad de ancho de banda por parte de nuevos servicios y aplicaciones, en especial las basadas en gráficos. (Pinillos, 2003)

Por esta razón, los routers deben tener la capacidad de reenviar los datagramas IP de manera rápida y así afrontar velocidades inmensas y el incremento de carga lo más rápido y eficiente posible. Para esto es necesario plataformas de hardware robustas, así como también es importante el diseño IP que se tenga. El protocolo de internet versión 6 (IPv6) ofrece tres aspectos de diseño que contribuyen a mejorar el rendimiento de las interredes:

- La simplificación de la cabecera IP. Se reducen los trece campos presentes en IPv4 a sólo ocho campos. Esto permite a los routers procesar con mayor rapidez los paquetes y mejorar el rendimiento. [Lázaro & Miralles, 2004]
  [Lázaro & Miralles, 2004] Mayor eficiencia en el uso de los campos en la cabecera del paquete. Este cambio fue esencial, ya que algunos capos que antes eran obligatorios ahora son opcionales. Además, la representación de las opciones es diferente, haciendo más sencillo que los routers hagan caso omiso de opciones no dirigidas a ellos, mejorando así el tiempo de procesamiento de paquetes. [Lázaro & Miralles, 2004]
- La cabecera del paquete IPv6 es de longitud fija mientras que la cabecera de IPv4 es de longitud variable, simplificando una vez más el proceso. [Lázaro & Miralles, 2004]
- La fragmentación no se permite en lo routers IPv6. Solo puede ser realizada por el origen. [Lázaro & Miralles, 2004]

c. **Servicios de red:** (Pinillos, 2003) IPv6, cuenta con un mecanismo que permite a un transmisor y un receptor establecer una trayectoria de alta calidad por la red y asociarle los datagramas, garantizando el alto desempeño a aplicaciones de audio y video en tiempo real. IPv6 permite el etiquetado de los paquetes que pertenecen a un flujo de tráfico en particular para la cual el origen solicita un manejo especial.

d. **Capacidad de seguridad:** (Pinillos, 2003) IPv6 proporciona soporte nativo para seguridad basándose en sus cabeceras de extensión. Por medio de las cabeceras de autenticación y la cabecera de encapsulamiento seguro, se logra provee

e. **Diferentes niveles de seguridad para diferentes usuarios.** Esto es muy importante ya que diferentes comunidades de usuarios tienen diferentes necesidades de seguridad.

f. **Calidad de Servicio:** (Pinillos, 2003) La calidad de servicio en IPv6, es un servicio más robusto que el provisto por datagrama llamados, Prioridad ("priority –4 bits-") y Etiqueta de Flujo ("Flow Label –24 bits-"). Estos, son usados para que un host pueda identificar los paquetes, para el cual se requiere un manejo especial por parte de los routers IPv6. Esta capacidad es importante, para el momento de soportar aplicaciones que requieren el menor grado de retardos, delay o alteraciones en el flujo. Estos tipos de aplicaciones son comúnmente descritas como aplicaciones multimedia o de tiempo real. [Blanchet, Marc. Migrating to IPv6, 2006]

4.4. Campos de la Cabecera IPv6

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

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

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

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

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

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

4. El cuarto campo es el de la longitud del campo útil, el cual está contenido de 16 bits, y define la longitud de lo que sigue después de la cabecera básica de IPv6, esto quiere decir que mide la longitud de la información del transporte, de la aplicación así como de las extensiones de la cabecera si hubieran. La máxima longitud del campo útil es de 216 = 65536 octetos.

5. El quinto campo es el de siguiente cabecera el cual está compuesto de 8 bits. Este campo identifica los datos que están dentro de la carga útil del

datagrama IP. Típicamente este es el protocolo de transporte (TCP o UDP) pero puede ser protocolos de encapsulamiento como ESP para IPsec. Este campo es el equivalente al del campo de Protocolo en IPv4 y comparte los mismos valores. El listado completo de los números de protocolos se puede encontrar en la página de IANA en la parte de números de protocolos.

6. El sexto campo es el de límite de saltos, el cual está compuesto de 8 bits, que fue implementado derivado de una sugerencia en el RFC791, como un contador de 28= 256, el cual va disminuyendo en una unidad cada vez que un enrutador envía el datagrama, hasta que su valor llega a cero, entonces se envía un mensaje ICMP de “tiempo excedido”.

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

4.4.1. Extensiones de la Cabecera IPv6

Las extensiones de la cabecera de IPv6 son una manera de manejar las opciones de IPv4 mejorando el procesamiento, estas extensiones se pueden colocar entre la cabecera IPv6 y la cabecera de capa superior siguiente dentro de un paquete. Cada extensión de cabecera es un múltiplo de 8 octetos de largo, para conservar la alineación de 8 octetos para las cabeceras subsiguientes y cada uno de los tipos de extensiones están identificadas por un valor específico del campo siguiente cabecera. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

Tabla N° 04: Valores de siguiente cabecera para las extensiones IPv6

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

Las cabeceras de extensión no son examinadas ni procesadas por ningún nodo a lo largo de la ruta de entrega de un paquete, hasta que el paquete alcance el nodo (o cada uno del conjunto de nodos, en el caso de multienvío) identificado en el campo Dirección Destino de la cabecera IPv6. Las extensiones de cabecera se deben de procesar únicamente en el orden en que vienen. El valor de la siguiente cabecera de la cabecera del datagrama IP está apuntando a la primera extensión (si hubiera), y esta extensión apuntando a la siguiente y así sucesivamente. Es por ello que cuando más de una extensión de cabecera se usa en un mismo paquete, se recomienda que esas cabeceras tengan un orden el cual está especificado en el RFC 2460 [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

Tabla N° 05: Orden de las extensiones de cabecera IPv6

Orden	Cabecera
1	IPv6
2	Opciones de salto a salto
3	Opciones de destino (Nota 1)
4	Enrutamiento
5	Fragmentación
6	Autenticación
7	Seguridad del encapsulado de carga útil (Nota 2)
8	Opciones de destino (Nota 3)
9	De capa superior

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

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

Nota 3, para las opciones a ser procesadas solo por el destino final del paquete. Cada cabecera de extensión debe ocurrir solamente una vez, a excepción de la cabecera Opciones de Destino la cual debe de ocurrir a lo sumo dos veces (una vez antes de una cabecera Enrutamiento y la otra vez antes de una cabecera de capa superior). Si la cabecera de capa superior es otra cabecera IPv6 (en el caso de que el IPv6 sea tunelizado o encapsulado en el IPv6), puede ser

seguida por sus propias cabeceras de extensión, las cuales están separadamente sujetas a las mismas recomendaciones de orden.

Los nodos IPv6 deben aceptar e intentar procesar cabeceras de extensión en cualquier orden y cualquier número de veces que ocurran en un mismo paquete, a excepción de la cabecera Opciones de Salto a Salto la cual está restringida a aparecer sólo inmediatamente después de una cabecera IPv6. No obstante, se aconseja fuertemente que los originadores de paquetes IPv6 se apeguen al orden recomendado arriba hasta y a menos que especificaciones subsiguientes corrijan esa recomendación. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

4.4.2. Salto a Salto

La opción salto a salto tiene que ser examinada por cada uno de los nodos intermedios, como por ejemplo enrutadores, que hay en todo el camino hasta el destino. Actualmente hay dos usos para esta extensión, la de alerta de enrutador y la de Jumbograma. La función de alerta de enrutador sirve para alertar a los nodos intermediarios que están a lo largo del camino para que procesen específicamente el datagrama, y así es una fácil manera en que los enrutadores pueden interceptar únicamente estos datagramas etiquetados sin sobrecargar el procesamiento de los mismos. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

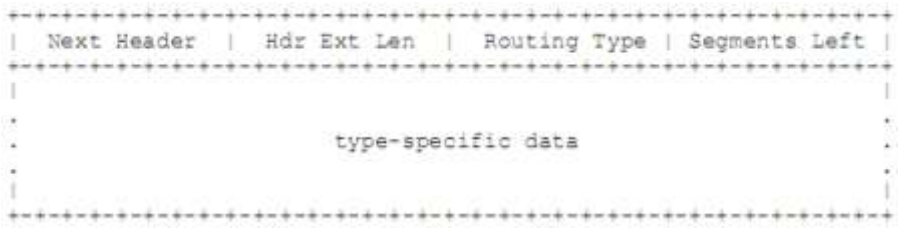
Los jumbogramas son datagramas de una longitud mayor de 64,000 octetos, los cuales necesitan de un procesamiento especial por todos los nodos intermedios como por ejemplo los enrutadores, debido a que son sobredimensionados comparados con el máximo de 16 bits de longitud del campo de carga útil. Un jumbograma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

- El campo de longitud de carga útil está fijo con un valor igual a 0.
- El campo siguiente cabecera está configurado con la opción salto a salto.
- La extensión salto a salto identifica a un jumbograma y contiene 32 bits especificando el tamaño del datagrama. De aquí que los jumbogramas tienen un tamaño máximo de 4Gigabits = 232.

4.4.3. Enrutamiento

La cabecera de enrutamiento es una lista en la cual se indica cuál o cuáles son los nodos que se visitarán para alcanzar el destino del paquete, ésta es muy parecida a opción de origen impreciso y registro de ruta de IPv4. El valor de identificación de esta extensión es de una cabecera siguiente igual a 43 (NH=43) [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

Imagen N° 23: Cabecera de enrutamiento



El campo cabecera siguiente identifica el tipo de cabecera que sigue inmediatamente a la cabecera de enrutamiento. El campo longitud de la extensión de la cabecera es un campo de 8 bits el cual mide la longitud de la cabecera de enrutamiento en unidades de 8 octetos. El campo de tipo de enrutamiento es un campo de 8 bits que identifica alguna variante en la cabecera de enrutamiento. El campo de segmentos pendientes es un campo de 8 bits que indica el número de nodos intermedios explícitamente pendientes de visitar antes de alcanzar el destino del paquete. El campo de tipo específicos de datos es un campo de longitud variable que depende del campo de tipo de enrutamiento y del campo de longitud tal que la cabecera de enrutamiento completa es un número entero múltiplo de 8 octetos de longitud.

Si mientras se procesa un paquete recibido, el nodo encuentra una cabecera de enrutamiento con un valor de tipo de enrutamiento desconocido, el comportamiento de este nodo dependerá del valor del campo segmentos pendientes tal como sigue; si el valor del campo de segmentos pendientes es cero, el nodo debe de ignorar la cabecera de enrutamiento y proceder a procesar la siguiente cabecera del paquete. Si el valor del campo de segmentos pendientes no es cero, el nodo debe de descartar el paquete y mandar un

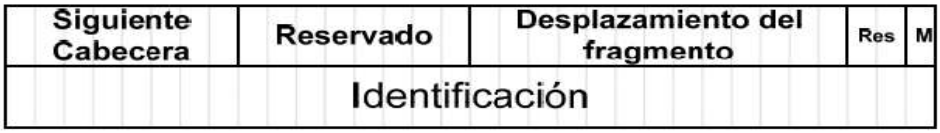
mensaje ICMP “problema de parámetro” con código 0, al nodo que originó el paquete indicando el tipo de enrutamiento desconocido.

Habiendo procesado una cabecera de enrutamiento, si un nodo intermedio determina que el paquete recibido será remitido hacia un enlace cuya MTU es menor que el tamaño del paquete, dicho nodo debe de descartar el paquete y enviar un mensaje ICMP “paquete demasiado grande” a la dirección origen del paquete. Una cabecera de enrutamiento no se examina o procesa hasta que alcance el nodo identificado en el campo de dirección destino de la cabecera IPv6. En dicho nodo al darle tratamiento al campo Siguiente Cabecera de la cabecera inmediatamente precedente ocasiona que la extensión cabecera de enrutamiento sea invocada. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

4.4.4. Fragmento

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

Imagen N° 24: Cabecera de fragmentación

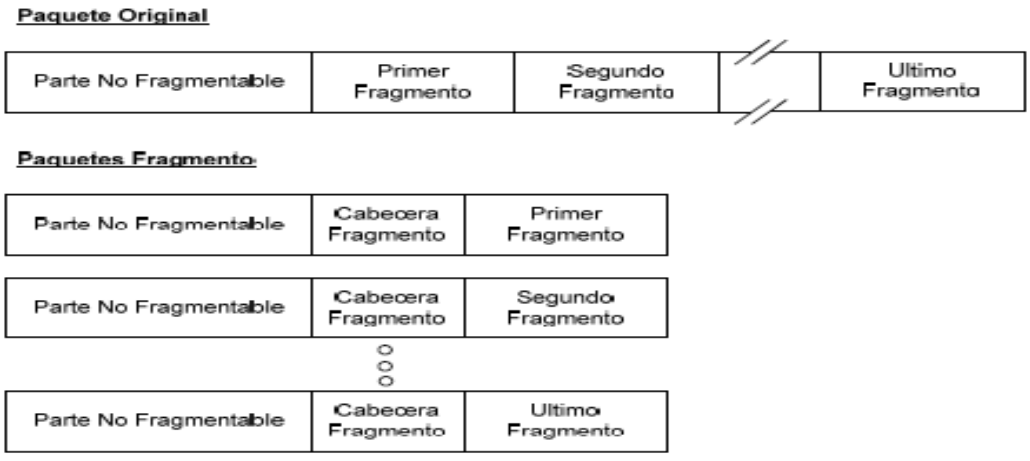


El campo siguiente cabecera, es de 8 bits, y es el que identifica el tipo de cabecera inicial de la parte fragmentable del paquete original. El campo reservado es de 8 bits, es un campo que se inicia en 0 para la trasmisión y es ignorado en la recepción. El campo desplazamiento del fragmento es un entero sin signo de 13 bits, el cual indica el desplazamiento en unidades de 8 octetos de los datos que siguen a esta cabecera en relación al inicio de la parte fragmentable del paquete original. El campo Res, es un campo de 2 bits, el cual también es inicializado en 0 para la transmisión y es ignorado en la recepción.

El campo M, es llamado Bandera M y es de 1 bit, el cual tiene como posibles valores 1= más fragmentos y 0=último fragmento.

El campo identificación es un campo de 32 bits, el cual es generado por el nodo origen para poder identificar a todos los paquetes que pertenecen al paquete original. Este campo es usualmente implementado como contador el cual se incrementa en una unidad por cada paquete que necesita ser fragmentado por el nodo origen. La identificación debe de ser diferente al de cualquier otro paquete fragmentado enviado recientemente (recientemente significa dentro del máximo tiempo de vida probable de un paquete, incluyendo el tránsito del origen hacia el destino y el tiempo gastado esperando el reensamblaje con otros fragmentos del mismo paquete) con la misma dirección origen y destino.
El paquete inicialmente sin fragmentar es llamado paquete original, el cual está compuesto de dos partes, la primera es la parte no fragmentable y la segunda es la parte fragmentable. La parte no fragmentable consiste de la cabecera IPv6 más alguna extensión que debe ser procesada por los nodos a lo largo de toda la ruta hasta alcanzar el destino. La parte fragmentable consiste en cualquier extensión de la cabecera que necesita ser únicamente procesada por el nodo destino más las cabeceras de capas superiores y cualquier otrodato. Los fragmentos se trasmiten por separado en paquetes fragmento.

Imagen N° 25: Paquete original y fragmentos



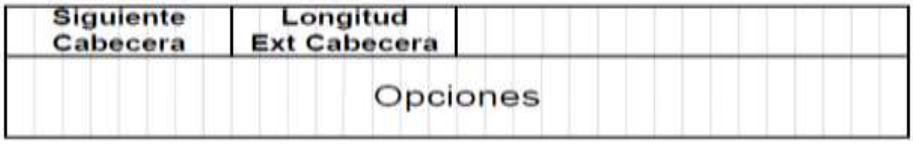
El nodo destino reúne todos los fragmentos y los reensambla. Los fragmentos deben de tener la misma dirección de destino y de origen y el mismo valor de ensamblaje para poder reensamblarlos. Si todos los fragmentos no son

recibidos por el destino dentro de los 60 segundos transcurridos después de haber recibido el primer fragmento, el nodo destino descartará todos los paquetes. Si el nodo destino ya había recibido el primer fragmento (el cual tendrá desplazamiento = cero), enviará de regreso al nodo origen un mensaje ICMPv6 “Tiempo de reensamblaje de fragmento excedido”.

4.4.5. Opciones de destino

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

Imagen N° 26: Cabecera opciones de destino



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

4.5. Arquitectura del Protocolo de Internet versión 6 (IPv6)

La arquitectura de IPv6 es una versión mejorada de IPv4, sin modificar demasiado la estructura ni contenido, pero con cambios sustanciales en seguridad y retirando datos innecesarios o redundantes, dichos cambios se debieron a 20 años de experiencia con IPv4. La arquitectura IPv6 está conformada por una cabecera de 40 bytes fijos, una cabecera de extensión opcional que no es adicionada a la cabecera fija sino que se agrega a la carga útil en caso sea utilizada. La nueva estructura de la cabecera del protocolo IP versión 6 se caracteriza principalmente por dos particularidades:

a. Ampliar el campo de dirección IP, es decir, de 32 bits se aumenta a 128 bits cada dirección.
b. Utilizar campos de longitud fija, facilitando así el proceso de cada datagrama en los ruteadores.

CAPÍTULO V

ESTRATEGIA DE MIGRACIÓN DE IPv4 A IPv6

V. ESTRATEGIA DE MIGRACIÓN DE IPv4 A IPv6.

IPv6 ha sido diseñado de tal forma que se facilite la migración y la coexistencia con IPv4. Dicha coexistencia con IPv4 puede tardar algunos años, motivo por el cual se han desarrollado varios mecanismos de transición. Existen tres principales categorías de mecanismos de transición. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

- Doble pila
- Túnel
- Traducción IPv4 a IPv6

Estos mecanismos de transición pueden ser utilizados solos o en combinación. La migración a IPv6 puede ser realizada paso a paso, comenzando con un nodo o con una subred. También puede darse el caso en que la red sea migrada a IPv6, mientras que nuestro proveedor de servicios (ISP) siga utilizando IPv4 o viceversa. En este contexto de migración a IPv6, surgen nuevos términos con los cuales se designa a ciertos tipos de nodos, los cuales son:

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

5.1. DOBLE PILA

Este tipo de mecanismo es aquel en el que se tendrá un soporte completo en los nodos así como en los enrutadores para los dos protocolos IPv4 e IPv6. A este tipo de nodo se les denomina nodos IPv6/IPv4, y tienen la habilidad de enviar y recibir los dos tipos de paquetes IPv4 e IPv6, lo cual les permite interoperar directamente con nodos IPv4 usando paquetes IPv4, y además interoperar con

nodos IPv6 usando paquetes IPv6. Una pila que ha sido habilitada, tiene una dirección IP asignada, de aquí que un nodo IPv6/IPv4 puede operar en tres modos distintos:

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

Dado que los nodos soportan ambos protocolos, dichos nodos adquieren sus direcciones con sus propios métodos, por ejemplo para obtener su dirección IPv4 utiliza DHCP, y el mismo nodo para obtener su dirección IPv6 utiliza DHCPv6.
El DNS (*Domain Name Server*) es utilizado en los dos protocolos para resolver nombres y direcciones IP. Un nodo IPv6/IPv4 necesita un DNS que sea capaz de resolver los dos tipos de registros de direcciones. El registro DNS “A” es usado para resolver direcciones IPv4 y el registro DNS “AAAA” o “A6” es usado para resolver direcciones IPv6. Si el host que se está resolviendo es de doble pila, entonces el DNS debe devolver los dos tipos de direcciones IP Una red de doble pila es una infraestructura en la cual la transmisión de ambos protocolos IPv4 e IPv6 está habilitada en los enrutadores. La desventaja es que se deben de tener tablas de enrutamiento para ambos protocolos, y además soporte para ambos protocolos. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009].

5.2. Túneles IPv6 sobre IPv4

Los túneles son una manera de utilizar la infraestructura de enrutamiento IPv4 existente para llevar el tráfico IPv6, hasta el momento en que se cuente con toda la infraestructura IPv6, o sea hasta que toda la red se haya migrado a IPv6. Los túneles pueden ser usados para llevar tráfico IPv6 encapsulándolo en paquetes IPv4 y tunelizándolo a través de toda la infraestructura de enrutamiento IPv4. Un túnel tiene dos puntos finales, el primero es el punto de entrada y el segundo es el punto de salida. El túnel puede ser implementado en diferentes maneras:

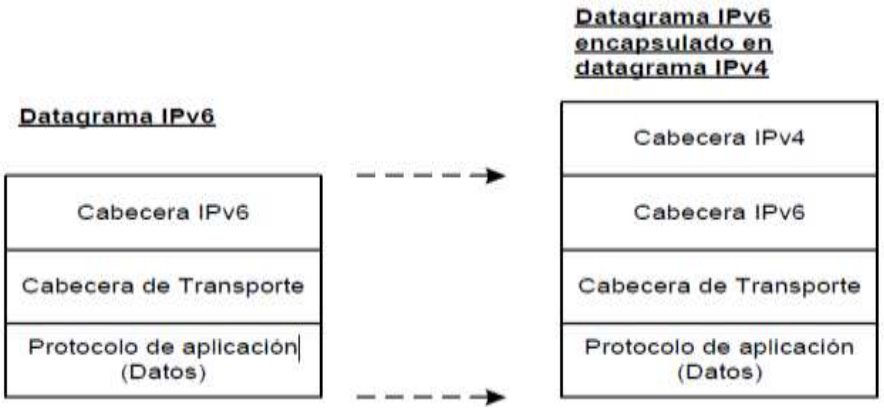
- Enrutador a enrutador. Los enrutadores IPv6/IPv4 interconectados por una infraestructura IPv4 pueden tunelizar paquetes IPv6 entre ellos.

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

❖ Encapsulamiento

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

Imagen N° 27: Encapsulamiento de un datagrama IPv6



La dirección IPv4 origen y destino del datagrama IPv4 son las direcciones del nodo encapsulado y desencapsulado, las cuales pueden ser o no las direcciones IPv6 origen y destino del datagrama IPv6. Los pasos del encapsulamiento de un paquete IPv6 son los siguientes:

- El punto de entrada del túnel (el encapsulador) decrementa el campo IPv6, límite de saltos, en una unidad, encapsula el paquete IPv6 en la cabecera IPv4, y transmite el paquete encapsulado a través del túnel. Si fuera necesario el paquete IPv4 es fragmentado.

- El punto de salida del túnel (el desencapsulador) desencapsula el paquete. Si el paquete fue fragmentado, lo reensambla. Luego el punto de salida remueve la cabecera IPv4 y procesa el paquete IPv6 a su destino original.

5.2.1. Túnel automático

Los túneles automáticos permiten a los nodos IPv6/IPv4 comunicarse por medio de la infraestructura IPv4 sin la necesidad de una pre configuración del túnel. La dirección del punto final del túnel está determinado por la dirección compatible IPv4 destino. Este tipo de dirección IPv6 es asignada exclusivamente a los nodos que utilizan túneles automáticos. Una dirección IPv4 10.12.83.119, tiene como dirección IPv4 compatible ::10.12.83.119, dirección IPv6 en la cual lo que se ha hecho es agregar un prefijo de 96 bits en el cual todos los bits son ceros. La interface a la cual la dirección IPv4 compatible está asignada es llamada comúnmente pseudointerface. Mientras que la dirección IPv4 utilizada no sea una dirección privada, la dirección IPv4 compatible será globalmente única. El túnel automático es creado con la extracción de la dirección IPv4 de la parte baja de la dirección IPv4 compatible.

Una tabla especial de enrutamiento puede ser utilizada para dirigir los paquetes a través del túnel. La ruta será una simple entrada de un prefijo de ceros con una máscara de 96 bits. Todos los paquetes con una dirección IPv4 compatible como dirección IPv6 destino coincidirán con el prefijo y serán enviados por el túnel automático. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

5.2.2. Túnel manual

Los túneles manuales o estáticos requieren que sean configurados en ambos puntos finales, las direcciones origen y destino IPv4 e IPv6, además que los nodos de los puntos finales deben de tener doble pila. Los túneles estáticos tienen algunos requerimientos. El primer requerimiento es que los dos enrutadores deben de ser doble pila. El segundo requerimiento es que el

enrutador de entrada debe de contar con una dirección IPv4 con la cual pueda alcanzar al enrutador de salida y viceversa.
Pero los túneles manuales tienen sus desventajas, una de ellas es que si son varios túneles los que hay que configurar, este trabajo puede ser pesado. Además si las direcciones IP están cambiando para varios túneles el trabajo también se convierte en pesado.
Este tipo de túnel puede ser utilizado cuando se necesitan sólo pocos túneles y cuando no está presente el NAT de IPv4. [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

5.3. Traducción IPv4 a IPv6

Este mecanismo de transición permite a un nodo que solo cuenta con el stack IPv6 comunicarse con otro nodo que solo tiene el stack IPv4. Sin embargo, ésta técnica requiere tener habilitados mecanismos de traducción entre IPv4 e IPv6 en los enrutadores de ambas redes. La principal desventaja es que todo el peso de este mecanismo de transición recae en los dispositivos encargados de hacer dicha traducción, a los que no siempre se tiene acceso. 6to4 es un mecanismo (RFC 3056) para que los sitios IPv6 puedan comunicarse entre sí, utilizando la red IPv4, sin la necesidad de contar con un túnel explícito.

En este mecanismo surgen nuevas definiciones:

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

CAPÍTULO VI

REALIDAD DE LA RED TELEMÁTICA DE LA UNPRG

VI. REALIDAD DE LA RED TELEMÁTICA DE LA UNPRG

Equipos con los que cuenta la red telemática de la Universidad Nacional Pedro Ruiz Gallo.

❖ **Agenda**

Introducción a los equipos de Comunicación Cisco a instalar.

- Introducción a la Plataforma Microsoft a instalar.
  – Active Directory
  – Exchange 2000 Server
  – Internet Security and Acceleration Server 2000
- Diseño físico de la Red en UNPRG.
- Diseño lógico de la Red en UNPRG.
- Configuración de servidor DC001
- Configuración de servidor DC002
- Configuración de servidor MAIL001
- Configuración de servidor ISA001
- Configuración de servidor DB001

6.1. Introducción a los Equipos de Comunicación CISCO a Instalar

Existen 2 modelos de switches CISCO: 4500 y 2950.

- El 4500 (Switch Core) es un switch Capa 2/3/4, maneja un backplane de 64 Gbps, 32000 Mac adresses, QoS, VTP, 4096 VLANs, entre otros.

- El 2950 (Switch de borde) maneja un backplane de 13.6 Gbps, 8000 Mac adresses, QoS, VTP, 250 VLANs, entre otros.

- El PIX 515E, posee 4 interfaces Ethernet para la red externa, interna y zonas DMZ, procesamiento de inspección de paquetes a 175 Mbps, manejo de NAT y PAT.

- El IDS 4215, posee 4 interfaces de sniffing 10/100 BaseTX,una capacidad de inspección de 80 Mbps, protección de ataques DNS, SMTP, IP Fragment.

- El Router 2611X, posee un puerto LAN y un puerto WAN, maneja protocolos de red Ethernet, Frame Relay, PPP, ISDN, entre otros.

- El backbone (entre switch principal y secundarios) es de F.O., corriendo con tecnología GigabitEthernet – 1 Gbps.

- Los enlaces entre switches de un mismo Closet de Comunicaciones, son mediante Stacking – 1 Gbps. Esto evita crear cuellos de botella al momento de salir al backbone.

- Los enlaces entre terminales de pabellón son switcheados y corren con tecnología FastEthernet –10/100 Mbps.

- Los enlaces de cada servidor al Switch Core serán a 1 Gbps, con cable UTP, para evitar los cuellos de botella.

6.2. Introducción a la Plataforma Microsoft a Instalar

Active Directory

- Parte integral de Windows 2000 Server
- Pemite una administración centralizada.
- Es un repositorio confiable de datos para la autenticación.
- Permite una organización jerárquica de la institución.
- Simplifica la administración de Windows 2000.
- Fortalece la seguridad de Windows 2000.
- Soporte Replicación Multi-Maestro.
- Los objetos del Directorio tienen atributos.

Exchange 2000 Server

- Plataforma de mensajería y colaboración.
- Integrado con Active Directory, un solo punto de administración.
- Maneja múltiples bases de datos de mensajes.
- Soporta Clustering.
- Encaminamiento SMTP tolerante a fallos
- Integrado a la seguridad de Windows 2000.

- Acceso universal: outlook, internet explorer.
- Integración con Office 2000/XP.

Internet Security and Acceleration Server

- Conexión segura, proteje la red interna del negocio.
- Mayor velocidad de navegación.
- Reducción en costos de Anchos de Banda.
- Reducción de Stress en servidores web.
- Maneja políticas de acceso interno y externo.
- Permite conexiones desde Internet a la red Interna - VPN.
- Administración integrada con Windows 2000.
- RAM caching.
- Filtros inteligentes para aplicaciones.
- Publicación segura de servidores.

Imagen N° 28: Diseño Físico de la Red de la UNPRG

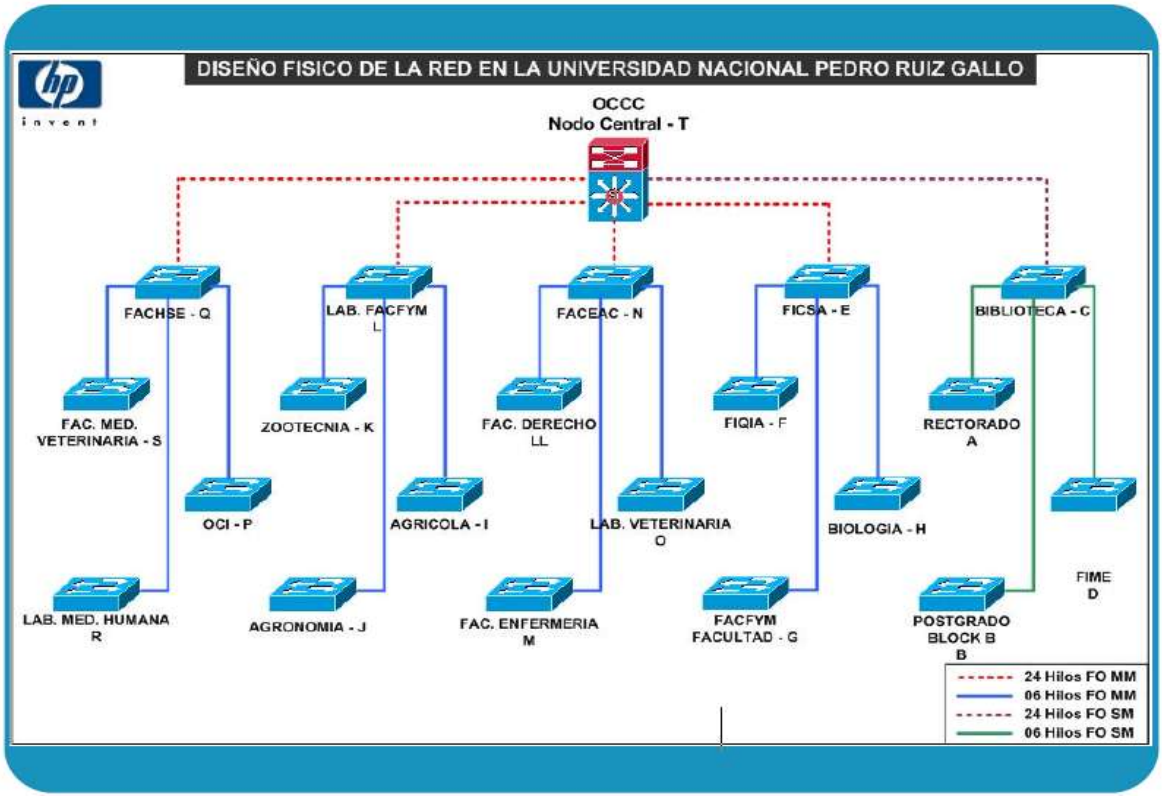


Imagen N° 29: Diseño Lógico de la Red de la UNPRG

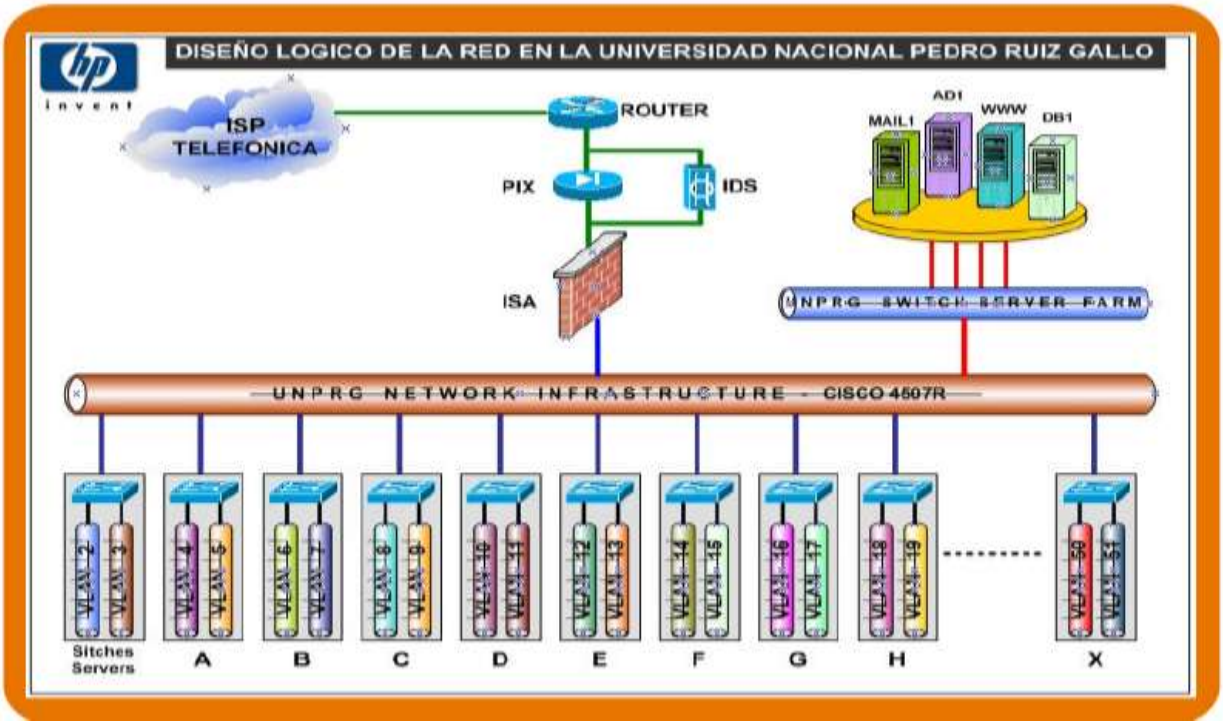
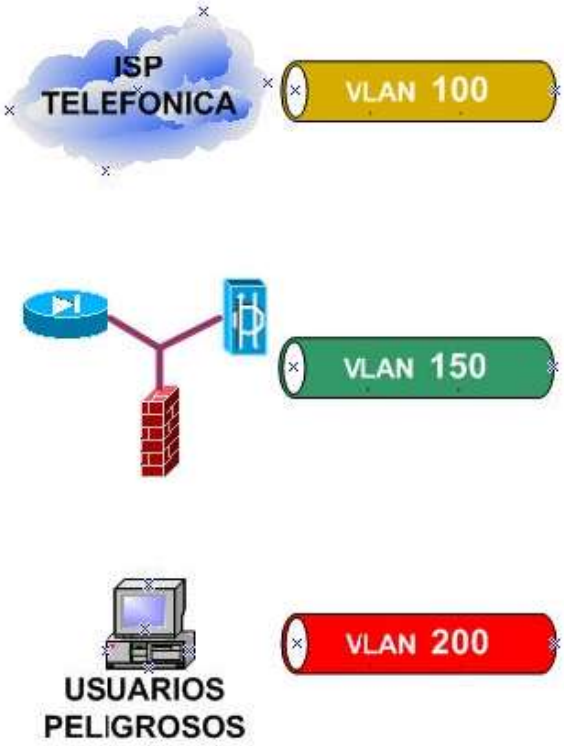


Imagen N°30: VLANs a crear en base a subredes por pabellón

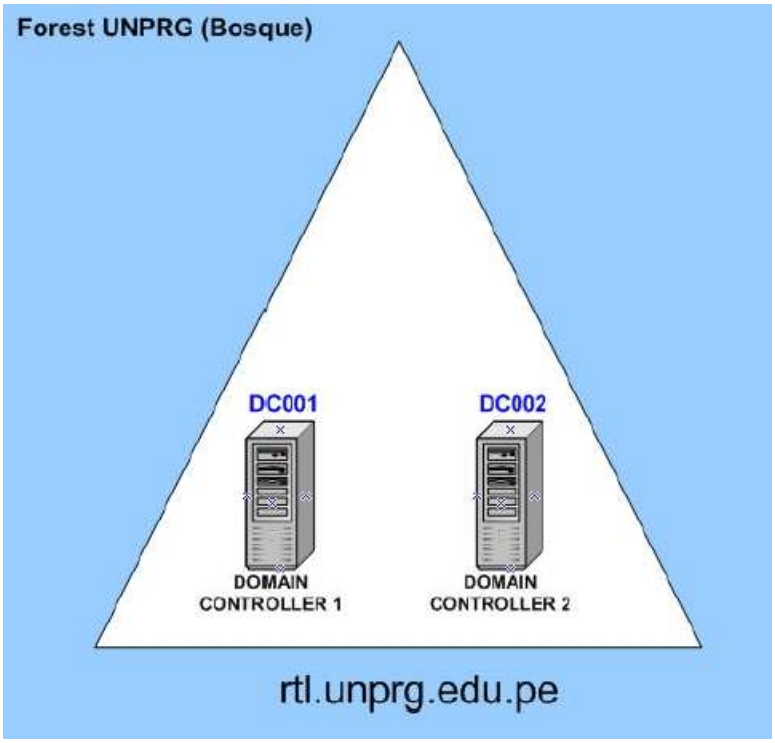
Imagen N° 31: VLANs a crear de Uso General



- ✓ **Configuración del Servidor DC001**

  Este servidor será el Controlador de Dominio Principal de la institución. También será el servidor DNS primario, servidor Weby servidor FTP. El nombre del dominio interno de la universidad será:
  Nombre DNS del dominio: rtl.unprg.edu.pe
  Nombre NetBIOS: UNPRG

Imagen N° 32: Organización Lógica del Directorio Activo



✓ **DNS:**

Se están manejando dos zonas DNS integradas al Directorio Activo. Estas son:

- **rtl.unprg.edu.pe**
  Es el nombre DNS que se le dará a la red interna, para evitar algún tipo de ataque externo.
- **unprg.edu.pe**
  Es el nombre DNS que se dará, para manipular el acceso al correo y web mediante un navegador de la red interna.

✓ **WEB y FTP:**

- El servidor alojará la página Web de la Universidad, mediante el servicio Internet Information Services. Los archivos estarán almacenados dentro de las carpetas:

- ✓ wwwROOT (web)
- ✓ ftpROOT (ftp)

- Con la finalidad de evitar ataques al directorio que se crea por default.
- Estos servicios estarán publicados en el servidor ISA.

Imagen N° 33: Configuración HW del Servidor DC001

HP Proliant DL380 G3			
Nombre	:	DC001	
Servicios	:	AD1 / DNS1 / WWW / FTP	
uPo	:	2 Xeón - 2.8 Ghz - 512 kb L2	
Ram	:	1 Gb	
Config. IP	:	IP Interno =	10.1.3.3/10.1.3.7
		Mask =	255.255.255.0
		DNS1 =	10.1.3.3
		DNS2 =	10.1.3.4
		Gateway =	10.1.3.2
HD	:	2 x 36.4Gb =	Raid 1 = 36.4 Gb
Config. HD:		NOS/AD =	c:\ 10 Gb
		Web/FTP =	d:\ 26.4 Gb

✓ **Configuración de Servidor DC002**

Este servidor será el Controlador de Dominio Secundario, cumpliendo las funciones de respaldo del DC001. También será el DNS secundario, con lo que la resolución de Nombres internos quedará respaldada por este servidor en caso de fallas del DNS primario.

System Insight Manager Software de gestión de Servidores y estaciones de trabajo HP, que permite el monitoreo de actividades críticas.

Imagen N° 34: Configuración HW del Servidor DC002

HP Proliant DL360 G3				
Nombre	:	DC002		
Servicios	:	AD2 / DNS2 / System Insight Manager		
uPo	:	1 Xeón - 2.8 Ghz - 512 kb L2		
Ram	:	1 Gb		
Config. IP	:	IP Interno	=	10.1.3.4
		Mask	=	255.255.255.0
		DNS1	=	10.1.3.3
		DNS2	=	10.1.3.4
		Gateway	=	10.1.3.2
HD	:	2 x 36.4Gb	=	Raid 1 = 36.4 Gb
Config. HD:		NOS/AD	=	c:\ 10 Gb
		SIM	=	d:\ 26.4 Gb

- ✓ **Configuración del Servidor MAIL001**

Se crearán 2 Storage Groups:

- Académica (contendrán las BD de mailbox de alumnos)
- Administrativa (contendrá las BD de mailbox de administrativos, docentes y directivos)

La configuración de los tamaños de los buzones se propone a continuación:

- 05 Mb para alumnos.
- 05 Mb para administrativos.
- 10 Mb para docentes.
- 10 Mb para directivos.

La dirección SMTP de todos los buzones es:

- **username@unprg.edu.pe**

✓ **DHCP:**

Debido al elevado número de estaciones de trabajo con el que cuenta UNC, la implantación del servicio DHCP es considerado esencial, de lo contrario, la asignación de direcciones IP en las estaciones requerirían de una gran inversión de tiempo y esfuerzo por parte del personal de soporte y administración de sistemas.

Para cada subred creada por pabellón se asignara el direccionamiento IP según las VLANs creadas en esas zonas. La configuración del servicio DHCP en UNPRG es como sigue:

- Rango de direcciones IP ofrecido a los usuarios por cada subred: 10.1.x.2 – 10.1.x.254
- Gateway: 10.1.x.1
- Máscara de red asignada: 255.255.255.0
- Servidores DNS principal: 10.1.3.3 - 10.1.3.4
- Sufijo DNS: rtl.unprg.edu.pe

Imagen N° 35: Configuración HW del servidor MAIL001

✓ **Configuración de Servidor ISA001**

Políticas de acceso:

La salida a Internet es libre, sólo pueden resolver protocolos CERN (http, https, ftp de lectura y gopher)

- El servicIo de correo está publicado hacia Internet, para el uso del Outlookk Web Access (OWA). Todos los correos entrantes están permitidos.
- El servicio web está publicado hacia Internet por el puerto 80 (más usado).
- Está habilitado el filtro de paquetes, solo pasan paquetes SMTP, DNS, y HTTP.

Opciones Habilitadas:

Estará instalado en modo Integrado: Firewall-ProxyCaching

- Está habilitado en Modo ARRAY, para la opción futura de particionar accesos.
- Está habilitado la opcion de CACHING normal y en Proxy-Reverso.
- Está habilitada la opción de RAM caching.
- Los accesos VPN están permitidos, sólo para usuarios autenticados.

Imagen N° 36: Configuración HW del servidor ISA001

HP Proliant DL360 G3			
Nombre	:	ISA001	
Servicios	:	Proxy / Firewall ADM/ACA	
uPo	:	1 Xeón - 2.8 Ghz - 512 kb L2	
Ram	:	1 Gb	
Config. IP	:	IP Externos =	10.100.10.10 - INT
			10.100.10.3 - Web
			10.100.10.5 - Mail
		Mask =	255.255.255.0
		DNS1 =	200.37.10.36
		DNS2 =	200.37.10.37
		Gateway =	10.100.10.1
		IP Interno =	10.1.3.2
		Mask =	255.255.255.0
		DNS1 =	10.1.3.3
		DNS2 =	10.1.3.4
HD	:	2 x 36.4Gb =	Raid 1 = 36.4 Gb
Config. HD:		NOS/ISA =	c:\ 10 Gb
		CACHE =	d:\ 26.4 Gb

- ✓ **Configuración de Servidor DB001**

Este servidor alojara a la Base de Datos de UNPRG, estará configurado para el trabajo con los otros servidores y quedara listo para la instalación del software que UNPRG considere conveniente.

Imagen N° 37: Configuración HW del servidor DB001

HP Proliant DL380 G3				
Nombre	:	DB001		
Servicios	:	Base de Datos		
uPo	:	2 Xeón - 2.8 Ghz - 512 kb L2		
Ram	:	1.5 Gb		
Config. IP	:	IP Interno	=	10.1.3.6
		Mask	=	255.255.255.0
		DNS1	=	10.1.3.3
		DNS2	=	10.1.3.4
		Gateway	=	10.1.3.1
HD	:	4 x 36.4Gb	=	Raid 5 = 109.2 Gb
Config. HD:		NOS	=	c:\ 10 Gb
		BD_Data	=	d:\ 99.2 Gb

Fuente: [Red telemática de la Universidad Nacional Pedro Ruiz Gallo]

CAPÍTULO VII

DISEÑO DE LA RED TELEMÁTICA DE LA UNPRG CON PACKET TRACER

VII. DISEÑO DE LA RED TELEMÁTICA DE LA UNPRG CON PACKET TRACER

7.1. Escenario

La Red Telemática de la Universidad Nacional Pedro Ruiz Gallo en la actualidad utiliza el protocolo de red IPv4 para el envío y recepción de datos. Por lo consiguiente se creará una red similar a la Red Telemática que actualmente presenta la Universidad para evaluar la seguridad integrada y la velocidad en dicho protocolo, y contrastarla con el protocolo de red IPv6 el cual no solo presenta más beneficios sino que es un protocolo orientado a la conexión y su nueva cabecera permite que sea más rápido que IPv4.

7.2. Finalidad del capítulo

- Evaluar el funcionamiento del protocolo de red IPv4 (no orientado a la conexión) y con respecto al protocolo de red IPv6 (orientado a la conexión).
- Evaluar la velocidad de IPv4 con respecto a IPv6.
- Elaborar una Red Telemática con ambos protocolos y demostrar su coexistencia.
- Lograr una Red Telemática más segura y más rápida.

7.3. Tabla de direccionamiento

Tabla N° 06: Tabla de Direccionamiento de la Red Telemática

DISPOSITIVO	INTERFAZ	VLAN	DIRECCION IP		MASCARA
Switch Core	Vlan 2	Vlan 2	IPv4	10.1.2.4	/24
			IPv6	2001:DB8:2::4	/64
Rectorado - A	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.8	/24
			IPv6		
	FastEthernet 1 - 12	Vlan 4	IPv4	10.1.4.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 5	IPv4	10.1.5.2	/24
			IPv6		
PostGrado - B	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.9	/24
			IPv6		
	FastEthernet 1 - 12	Vlan 6	IPv4	10.1.6.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 7	IPv4	10.1.7.2	/24
			IPv6		
Biblioteca - C	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.10	/24
			IPv6	2001:DB8:2::10	/64
	FastEthernet 1 - 12	Vlan 8	IPv4	10.1.8.2	/24
			IPv6	2001:DB8:8::2	/64
	FastEthernet 13 - 24	Vlan 9	IPv4	10.1.9.2	/24
			IPv6	2001:DB8:9::2	/64
FIME – D	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.11	/24
			IPv6		
	FastEthernet 1 - 12	Vlan 10	IPv4	10.1.10.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 11	IPv4	10.1.11.2	/24
			IPv6		
FICSA – E	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.12	/24
			IPv6		
	FastEthernet 1 - 12	Vlan 12	IPv4	10.1.12.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 13	IPv4	10.1.13.2	/24
			IPv6		

DISPOSITIVO	INTERFAZ	VLAN	DIRECCION IP		GATEWAY
FIQIA – F	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.13	/24
			IPv6		
	FastEthernet 1 -12	Vlan 14	IPv4	10.1.14.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 15	IPv4	10.1.15.2	/24
			IPv6		
FACFYM - G	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.14	/24
			IPv6		
	FastEthernet 1 -12	Vlan 16	IPv4	10.1.16.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 17	IPv4	10.1.17.2	/24
			IPv6		
Biología – H	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.15	/24
			IPv6		
	FastEthernet 1 -12	Vlan 18	IPv4	10.1.18.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 19	IPv4	10.1.19.2	/24
			IPv6		
Agricola – I	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.16	/24
			IPv6		
	FastEthernet 1 -12	Vlan 20	IPv4	10.1.20.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 21	IPv4	10.1.21.2	/24
			IPv6		
Agronomia - J	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.17	/24
			IPv6		
	FastEthernet 1 -12	Vlan 22	IPv4	10.1.22.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 23	IPv4	10.1.21.2	/24
			IPv6		
Zootecnia - K	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.18	/24
			IPv6		
	FastEthernet 1 -12	Vlan 24	IPv4	10.1.24.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 25	IPv4	10.1.25.2	/24
			IPv6		

DISPOSITIVO	INTERFAZ	VLAN	DIRECCION IP		GATEWAY
Lab. FACFYM - L	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.19	/24
			IPv6		
	FastEthernet 1 -12	Vlan 24	IPv4	10.1.24.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 25	IPv4	10.1.25.2	/24
			IPv6		
Fac. Derecho - LL	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.20	/24
			IPv6		
	FastEthernet 1 -12	Vlan 28	IPv4	10.1.28.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 29	IPv4	10.1.29.2	/24
			IPv6		
Fac. Enfermería - M	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.21	/24
			IPv6		
	FastEthernet 1 -12	Vlan 30	IPv4	10.1.30.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 31	IPv4	10.1.31.2	/24
			IPv6		
FACEAC – N	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.22	/24
			IPv6	2001:DB8:2::22	/64
	FastEthernet 1 -12	Vlan 32	IPv4	10.1.32.2	/24
			IPv6	2001:DB8:32::2	/64
	FastEthernet 13 - 24	Vlan 33	IPv4	10.1.33.2	/24
			IPv6	2001:DB8:33::2	/64
Lab. Veterinaria - O	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.21	/24
			IPv6		
	FastEthernet 1 -12	Vlan 34	IPv4	10.1.34.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 35	IPv4	10.1.35.2	/24
			IPv6		
OCI – P	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.21	/24
			IPv6		
	FastEthernet 1 -12	Vlan 36	IPv4	10.1.36.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 37	IPv4	10.1.37.2	/24
			IPv6		

DISPOSITIVO	INTERFAZ	VLAN	DIRECCION IP		GATEWAY
FACHSE - Q	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.19	/24
			IPv6	2001:DB8:2::19	/64
	FastEthernet 1 -12	Vlan 38	IPv4	10.1.38.2	/24
			IPv6	2001:DB8:38::2	/64
	FastEthernet 13 - 24	Vlan 39	IPv4	10.1.39.2	/24
			IPv6	2001:DB8:39::2	/64
Lab. Med. Humana - R	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.20	/24
			IPv6		
	FastEthernet 1 -12	Vlan 40	IPv4	10.1.40.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 41	IPv4	10.1.41.2	/24
			IPv6		
Med. Veterinaria – S	GigabitEthernet 1	Vlan 2	IPv4	10.1.2.21	/24
			IPv6		
	FastEthernet 1 -12	Vlan 42	IPv4	10.1.42.2	/24
			IPv6		
	FastEthernet 13 - 24	Vlan 43	IPv4	10.1.43.2	/24
			IPv6		

7.4. Configuración de la red telemática

7.4.1. Configuración básica

- **Paso 1: Entrar al Modo EXEC Privilegiado.**

  Router>**enable**
  Router#

- **Paso 2: Entrar al Modo de Configuración Global.**

  Router #**configure terminal**
  Router(config)#

- **Paso 3: Configurar el nombre del Router o Switch.**

  Router(config)#**hostname Core**
  Core(config)#

- **Paso 4: Configurar la contraseña de modo EXEC.**

  Core(config)#**enable secret IPv6**

- **Paso 5: Configurar la contraseña de consola en el Router o Switch.**

  Core(config)#**line console 0**
  Core(config-line)#**password IPv6**
  Core(config-line)#**login**
  Core(config-line)#**exit**

- **Paso 6: Configurar la contraseña para las líneas de terminal virtual.**

  Core(config)#**line vty 0 4**
  Core(config-line)#**password IPv6**
  Core(config-line)#**login**
  Core(config-line)#**exit**

- **Paso 7: Configurar un mensaje.**

  Core(config)#**banner motd &**
  Enter TEXT message. End with the character ´&´

  ****
  ******ACCESO RESTRINGIDO******
  ****
  &
  Core(config)#

7.5. Configuración de vlan

En la Tabla N° 07 encontraremos las VLAN creadas, y les asignaremos puertos.

Tabla N° 07: Asignación de puertos para las Vlan

SWITCH	PUERTOS	ASIGNACIÓN	RED
Switch Core	GigabitEthernet 1 FastEthernet 1 – 21	Enlace troncal 802.1q (VLAN 2 Nativa)	10.1.2.0
Rectorado – A	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 4	10.1.4.0
	FastEthernet 13 – 24	VLAN 5	10.1.5.0

SWITCH	PUERTOS	ASIGNACIÓN	RED
PostGrado – B	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 6	10.1.6.0
	FastEthernet 13 – 24	VLAN 7	10.1.7.0
Biblioteca – C	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 8	10.1.8.0
	FastEthernet 13 – 24	VLAN 9	10.1.9.0
FIME – D	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 10	10.1.10.0
	FastEthernet 13 – 24	VLAN 11	10.1.11.0
FICSA – E	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 12	10.1.12.0
	FastEthernet 13 – 24	VLAN 13	10.1.13.0
FIQIA – F	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 14	10.1.14.0
	FastEthernet 13 – 24	VLAN 15	10.1.15.0
FACFYM – G	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 16	10.1.16.0
	FastEthernet 13 – 24	VLAN 17	10.1.17.0
Biología – H	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 18	10.1.18.0
	FastEthernet 13 – 24	VLAN 19	10.1.19.0
Agrícola - I	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 20	10.1.20.0
	FastEthernet 13 – 24	VLAN 21	10.1.21.0
Agronomía – J	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 22	10.1.22.0
	FastEthernet 13 – 24	VLAN 23	10.1.23.0
Zootecnia – K	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 24	10.1.24.0
	FastEthernet 13 – 24	VLAN 25	10.1.25.0
Lab. FACFYM – L	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 26	10.1.26.0
	FastEthernet 13 – 24	VLAN 27	10.1.27.0
Fac. Derecho – LL	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 28	10.1.28.0
	FastEthernet 13 – 24	VLAN 29	10.1.29.0
Fac. Enfermería – M	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 30	10.1.30.0
	FastEthernet 13 – 24	VLAN 31	10.1.31.0

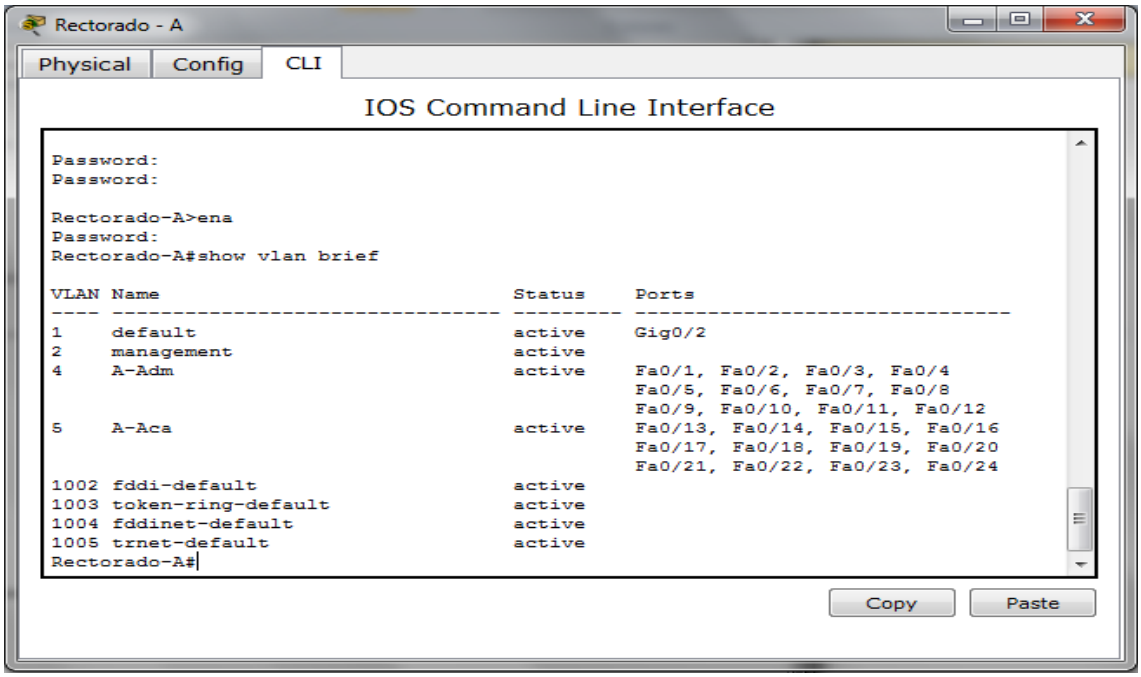
SWITCH	PUERTOS	ASIGNACIÓN	RED
FACEAC – N	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 32	10.1.32.0
	FastEthernet 13 – 24	VLAN 33	10.1.33.0
Lab. Veterinaria – O	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 34	10.1.34.0
	FastEthernet 13 – 24	VLAN 35	10.1.35.0
OCI – P	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 36	10.1.36.0
	FastEthernet 13 – 24	VLAN 37	10.1.37.0
FACHSE – Q	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 38	10.1.38.0
	FastEthernet 13 – 24	VLAN 39	10.1.39.0
Lab. Med. Humana – R	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 40	10.1.40.0
	FastEthernet 13 – 24	VLAN 41	10.1.41.0
Med. Veterinaria – S	GigabitEthernet 1	VLAN 2	10.1.2.0
	FastEthernet 1 – 12	VLAN 42	10.1.42.0
	FastEthernet 13 – 24	VLAN 43	10.1.43.0

- **Paso 1: Creación de VLAN en Switch**

  Rectorado-A (config)#**vlan 2**
  Rectorado-A (config-vlan)#**name management**
  Rectorado-A(config)#**vlan 4**
  Rectorado-A (config-vlan)#**name A-Adm**
  Rectorado-A(config)#**vlan 5**
  Rectorado-A (config-vlan)#**name A-Aca**

- **Paso 2: Verificación de creación de las VLAN**

  Rectorado-A (config)#**show vlan brief**



- **Paso 3: Asignar puerto del Switch a las VLAN y habilitar en modo acceso**

  Rectorado-A(config)#**interface range fa0/1-12**
  Rectorado-A(config-if-range)#**switchport access vlan 4**
  Rectorado-A(config-if-range)#**switchport mode access**
  Rectorado-A(config)#**interface range fa0/13-24**
  Rectorado-A(config-if-range)#**switchport access vlan 5**
  Rectorado-A(config-if-range)#**switchport mode access**
  Rectorado-A(config-if-range)#**end**

- **Paso 4: Asignar la VLAN de administración con IPv4**

  Rectorado-A(config)#**interface vlan 2**
  Rectorado-A(config-if)#**ip address 10.1.2.8 255.255.255.0**
  Rectorado-A(config-if)#**no shutdown**

- **Paso 5: Asignar la VLAN de administración con IPv6**

  Rectorado-A(config)#**interface vlan 2**
  Rectorado-A(config-if)#**ipv6 enable**

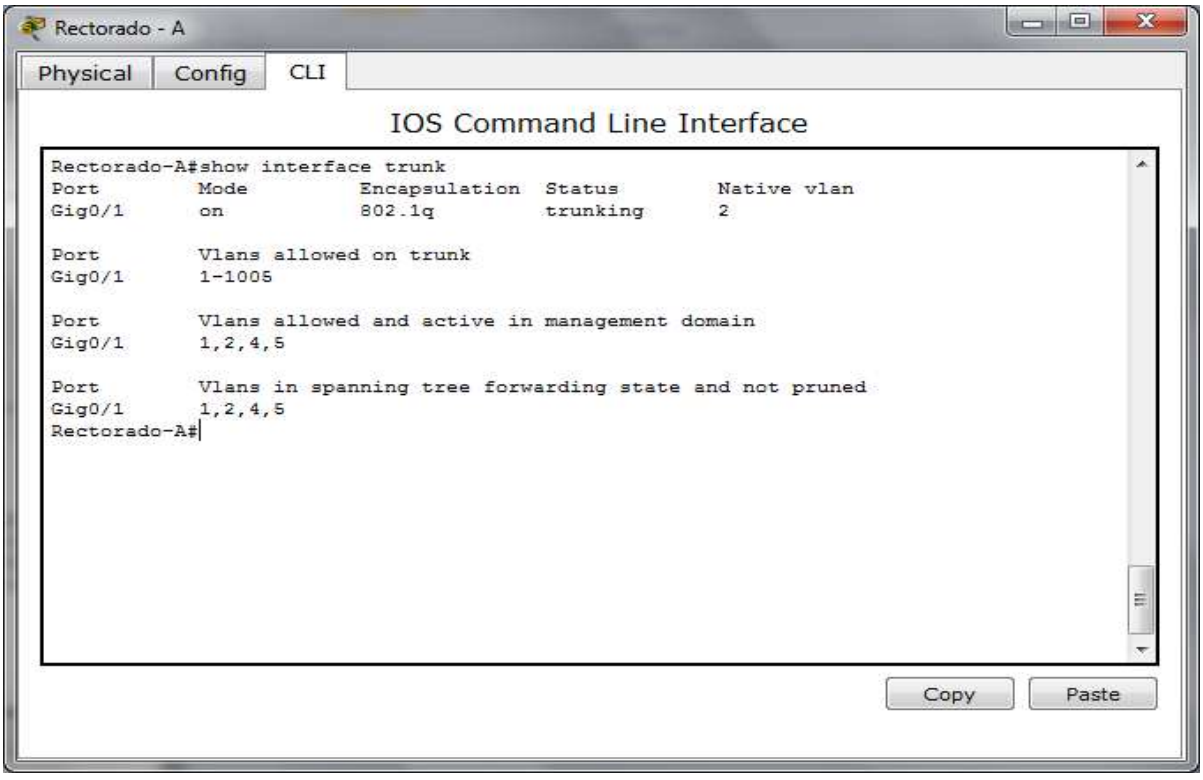
Rectorado-A(config-if)#**ipv6 address 2001:DB8:2::1/64**
Rectorado-A(config-if)#**no shutdown**

- **Paso 6: Configurar los enlaces troncales y la VLAN Nativa para los puertos de enlaces troncales en todos los Switches y el Router.**

  Rectorado-A(config)#**interface range GigabitEthernet 0/1**
  Rectorado-A(config)#**switchport trunk native vlan 2**
  Rectorado-A(config)#**switchport mode trunk**
  Rectorado-A(config)#**no shutdown**
  Rectorado-A(config)#**end**

- **Paso 7: Verificación de los enlaces troncales**

  Rectorado-A(config)#**show interface trunk**



7.6. Enrutamiento Inter VLAN

- **Paso 1: Configurar la interfaz de enlaces troncales en Router Core**

  Core(config)#**interface gigabitethernet 0/0**
  Core(config-if)#**no shutdown**
  Core(config-if)#**interface gigabitethernet 0/0.2**
  Core(config-subif)#**encapsulation dot1q 2**
  Core(config-subif)#**ip address 10.1.2.1 255.255.255.0**
  Core(config-if)#**interface gigabitethernet 0/0.3**
  Core(config-subif)#**encapsulation dot1q 3**
  Core(config-subif)#**ip address 10.1.3.1 255.255.255.0**
  Core(config-if)#**interface gigabitethernet 0/0.4**
  Core(config-subif)#**encapsulation dot1q 4**
  Core(config-subif)#**ip address 10.1.4.1 255.255.255.0**

- **Paso 2: Enrutamiento de VLAN con OSPF en IPv4**

  Core(config)#**router ospf 2**
  Core(config-router)#**network 10.1.0.0 0.0.0.255 area 2**

- **Paso 3: Enrutamiento de VLAN con OSPF en IPv6**

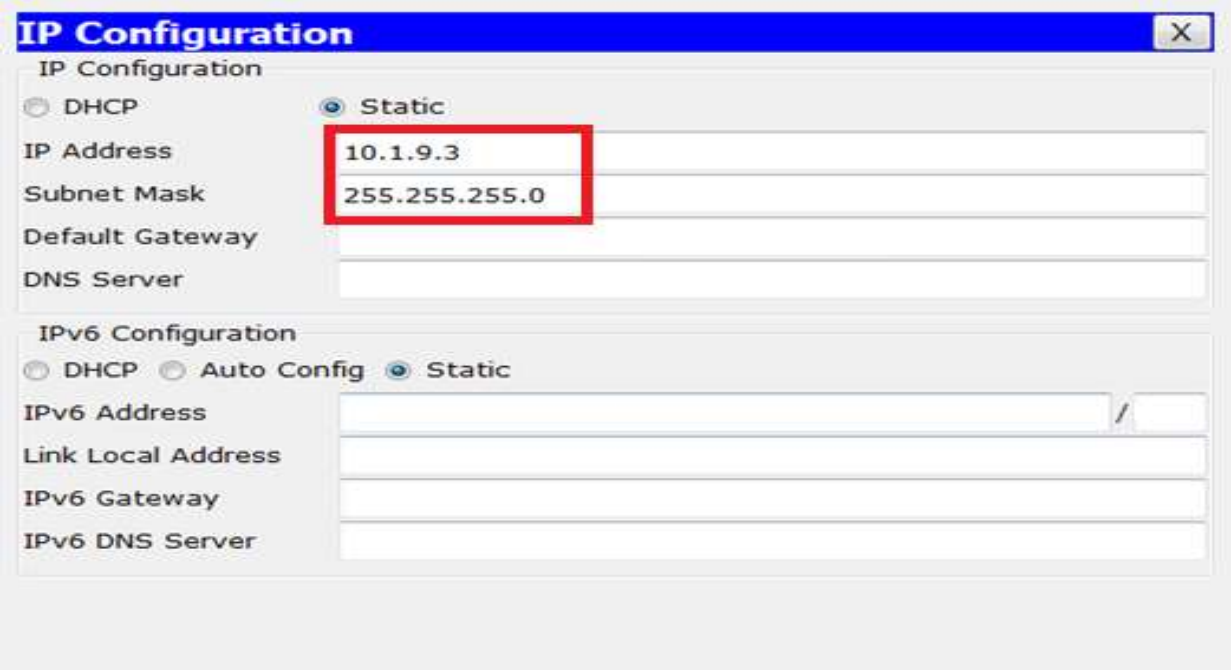
  Core(config)#**ipv6 unicast-routing**
  Core(config)#**ipv6 router ospf 1**
  Core(config-rtr)#**router-id 10.11.11.1**

- **Paso 4: Asignar enrutamiento IPv6 a las interfaces que utilizan dicho protocolo.**

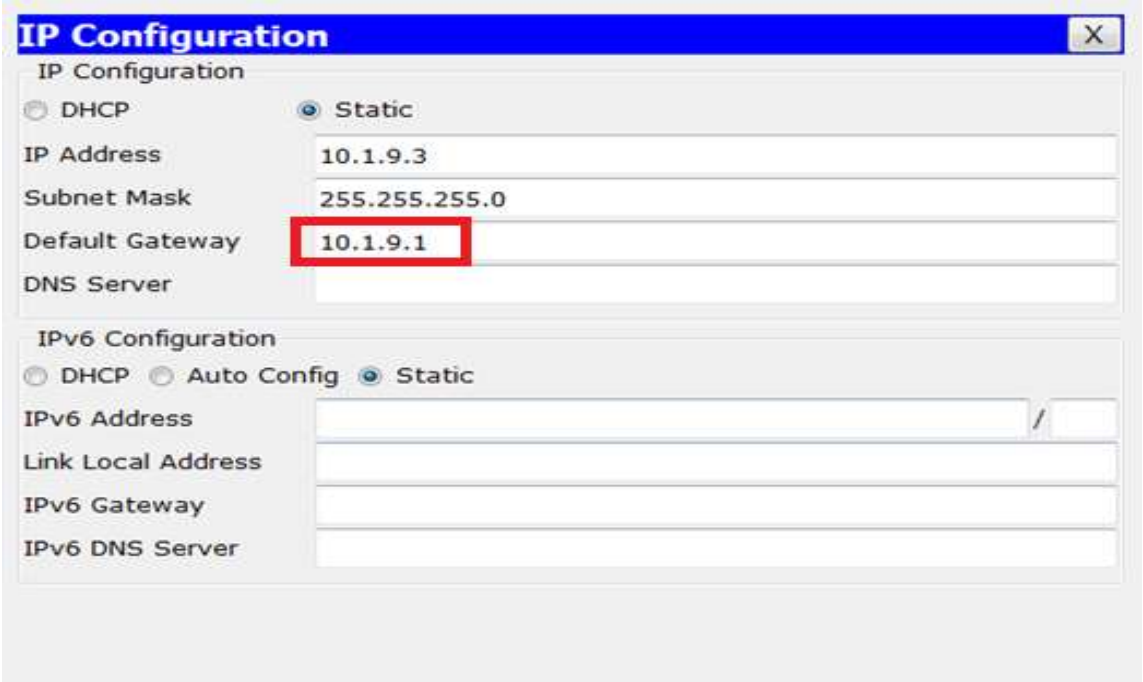
  Core(config)#**interface GigabitEthernet 0/0.2**
  Core(config-if)#**ipv6 ospf 1 area 0**

7.7. CONFIGURACIÓN DE PC

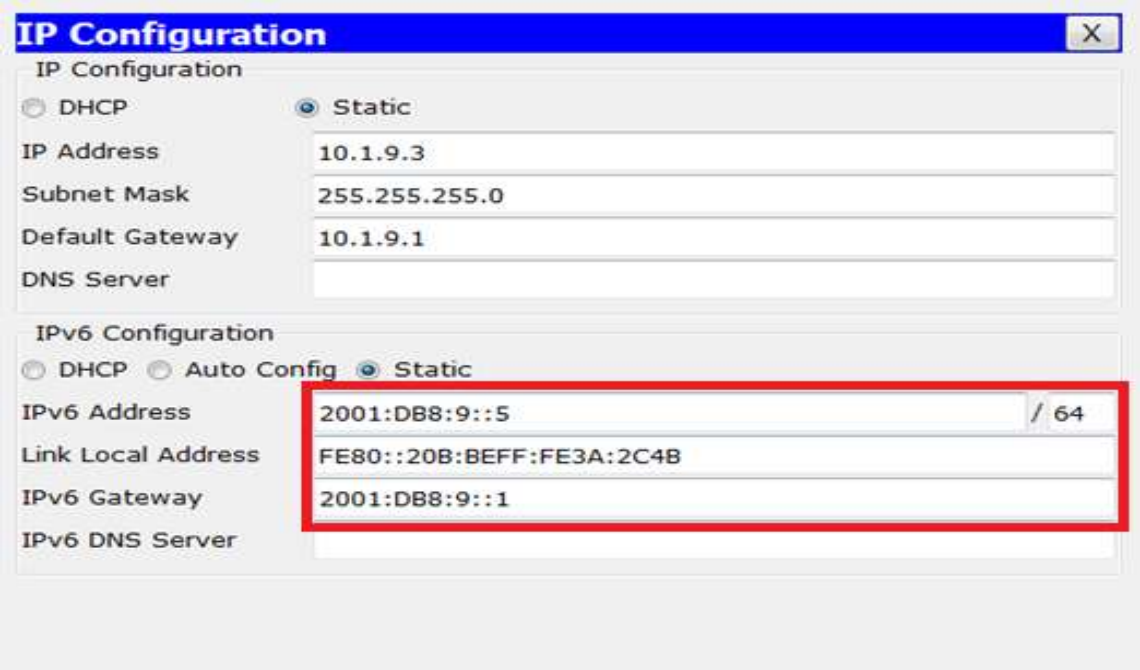
- **Paso 1: Asignamos la dirección IP para cada computadora.**



- **Paso 2: Asignamos el Puerta de Enlace Predeterminada (Gateway), de acuerdo a la red donde se encuentra la computadora.**



- **Paso 3: Asignamos la dirección IPv6 para cada computadora que se encuentra dentro de una red con protocolo IPv6.**



7.8. Mecanismo de transición dual stack

Se simuló la Red Telemática de la Universidad Nacional Pedro Ruiz Gallo, implementándola con nuevos Switch Capa 3 que soporte el protocolo de red IPv4 e IPv6 en una misma red, para realizar las pruebas de migración de acuerdo al Mecanismo de Transición Dual Stack.

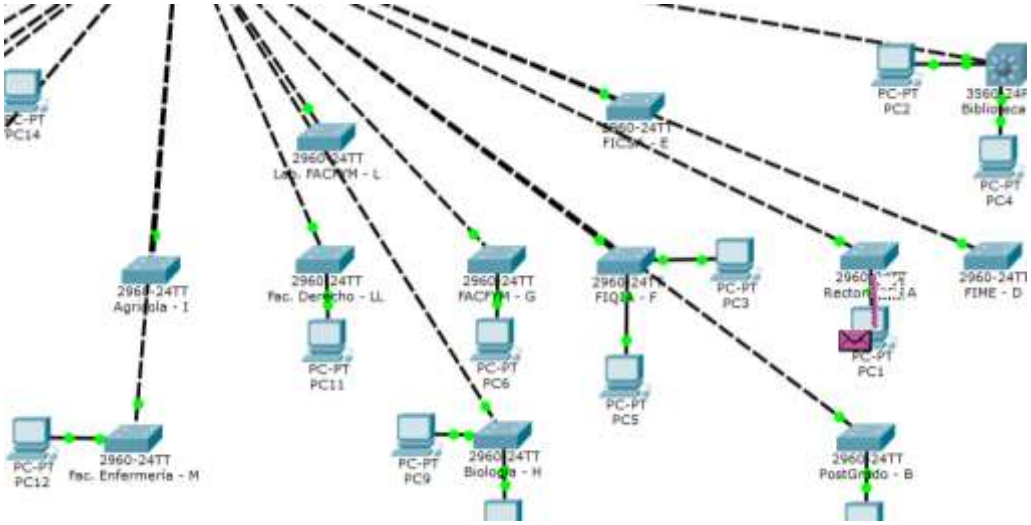
Luego de realizar la configuración de la Red Telemática se verificó la convivencia de ambos protocolos dentro de una misma Red; realizando pruebas entre Nodos IPv4, luego entre Nodos IPv6, y para terminar entre Nodos IPv4 e IPv6.

7.9. Red Telemática entre Nodos con IPv4

En la Red Telemática existen facultades con Nodos sólo IPv4, dentro de los cuales se hicieron pruebas realizando ping entre los hosts finales de estas subredes.

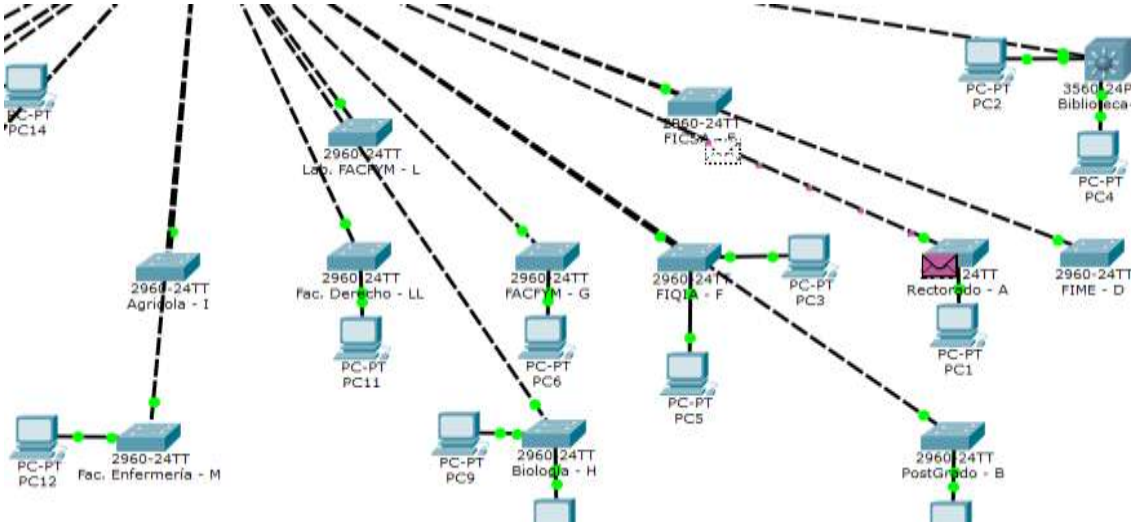
- Paso 1: La PC1 envía el Ping al Switch Rectorado – A (Ver Fig. N° 01)

Figura N° 01: Recepción del Ping de la PC1 al Switch Rectorado – A



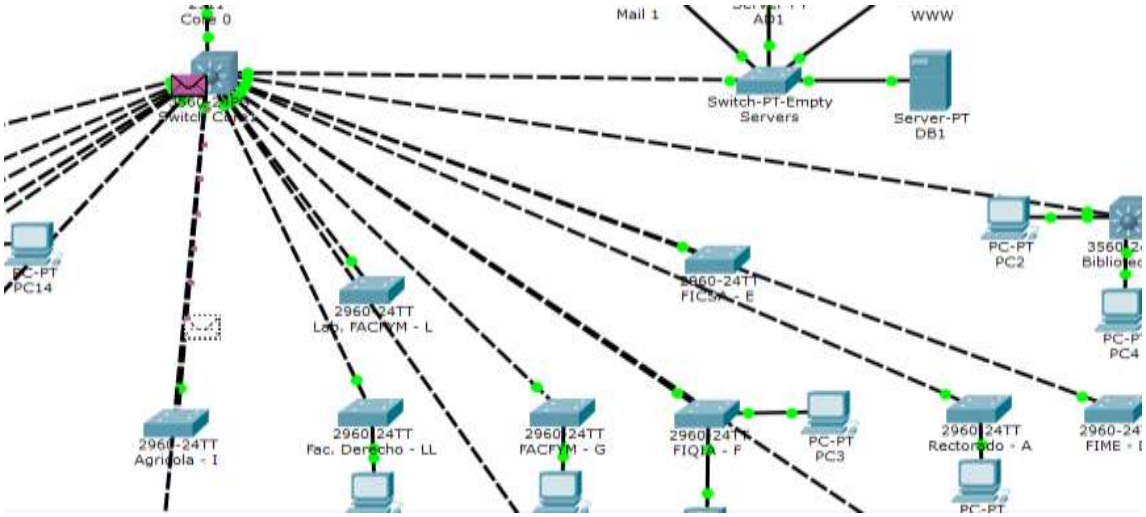
- Paso 2: El Switch Rectorado – A realiza el envío del Ping al Switch Core (Ver Fig. N° 02)

Figura N° 02: Envío del Ping del Switch Rectorado – A al Switch Core1



- Paso 3: El Switch Core1 realiza el envío del Ping al Switch Fac. Enfermería – M. (Ver Fig. N° 03)

Figura N° 03: Enrutamiento del Switch Core1 a la Fac. de Enfermería – M.



- Paso 4: El Switch Fac. Enfermería – M realiza el envío del Ping al Host de destino. (Ver Fig. N° 04)

Figura N° 04: Entre de Ping al Host Final (PC-12)

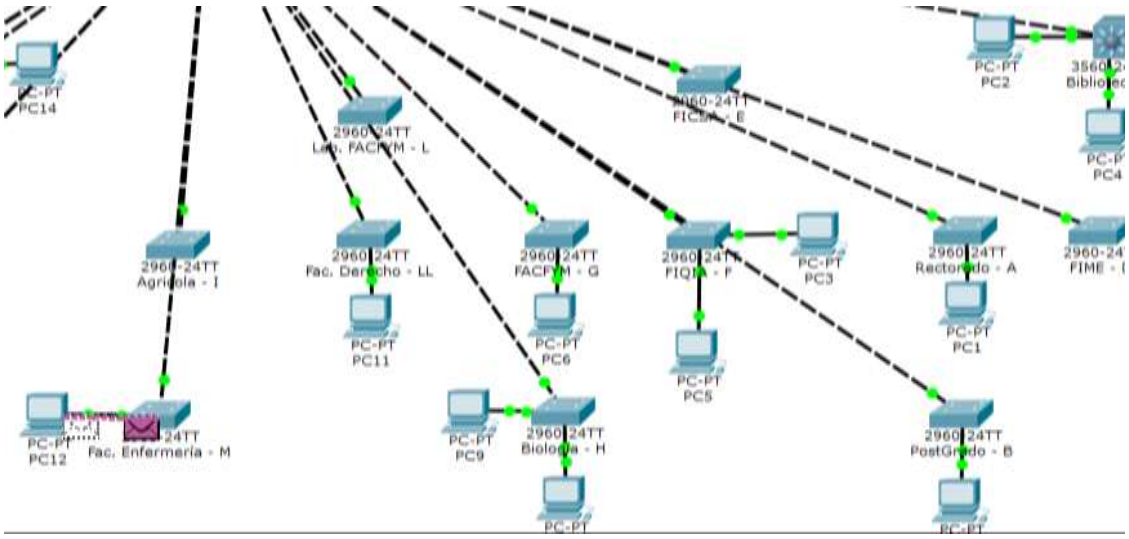


Figura N° 05: Ping exitoso entre nodos IPv4.

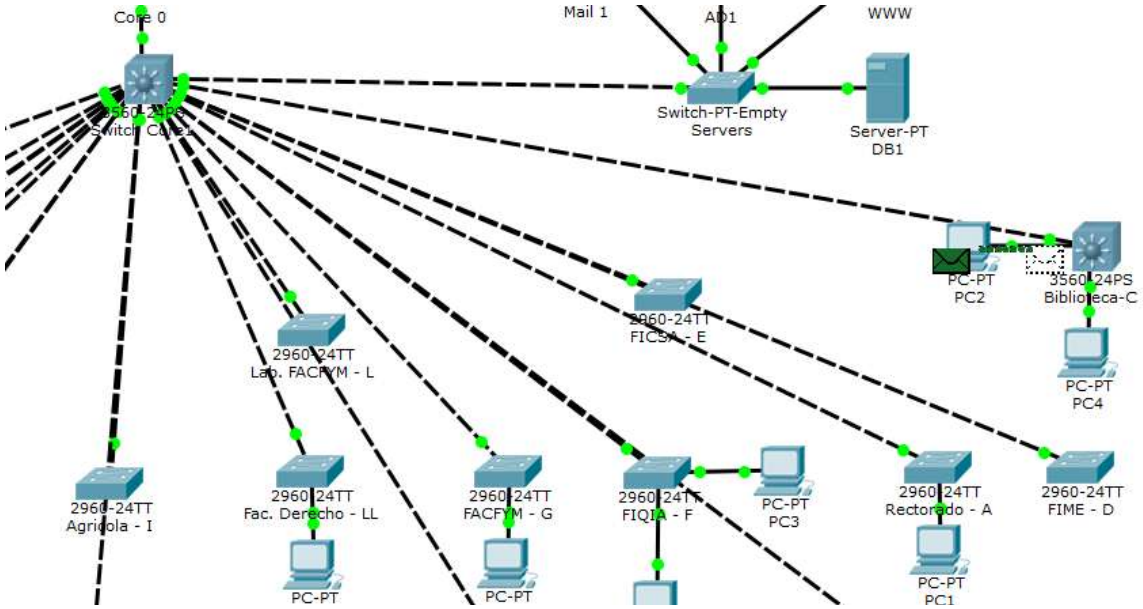
Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	PC1	10.1.30.5	ICMP		5.000	Y

7.10. Red Telemática entre Nodos con IPv6

En la Red Telemática también existen facultades con Nodos sólo IPv6, dentro de los cuales se hicieron pruebas realizando ping entre los hosts finales de estas subredes.

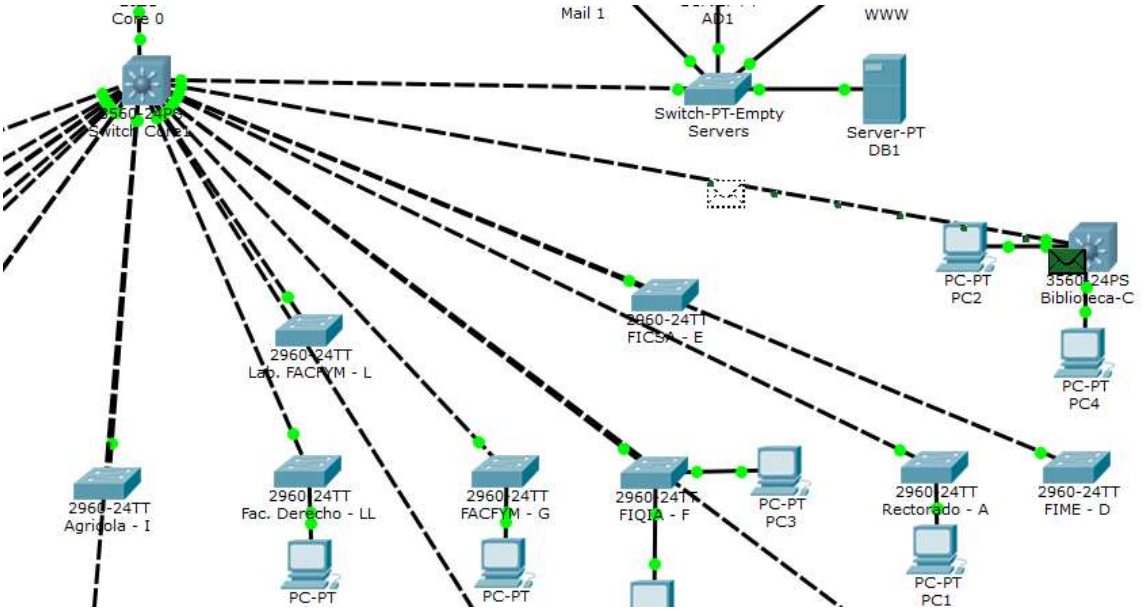
- Paso 1: La PC2 envía el Ping al Switch Biblioteca – C (Ver Fig. N° 06)

Fig. N° 06: Recepción del Ping de la PC2 al Switch Biblioteca – C



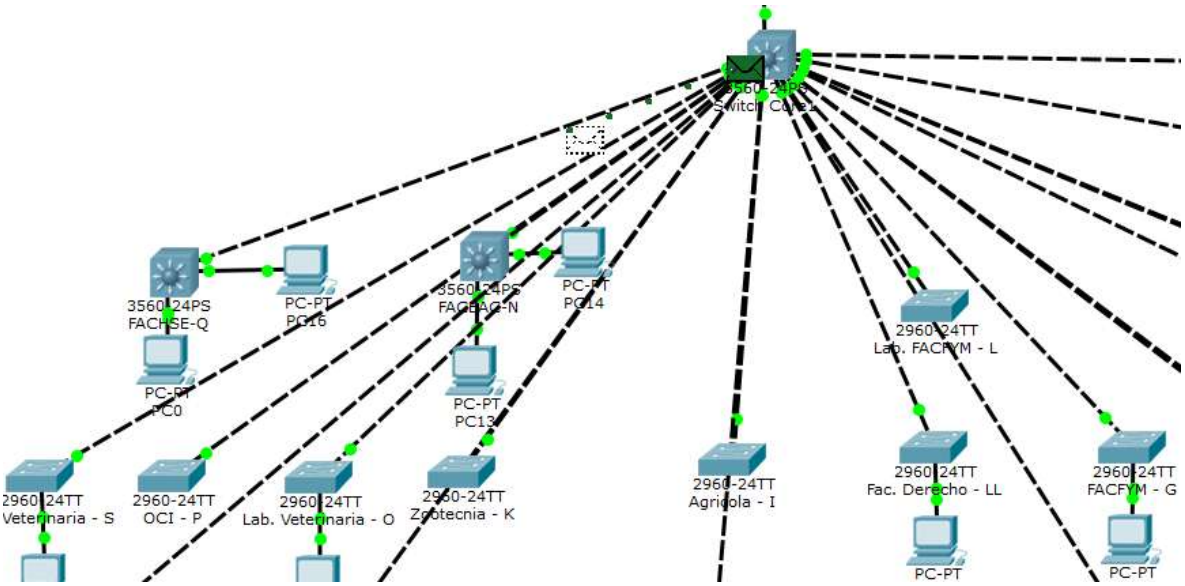
- Paso 2: El Switch Biblioteca – C realiza el envío del Ping al Switch Core (Ver Fig. N° 07)

Figura N° 07:: Envío del Ping del Switch Biblioteca – C al Switch Core1



- Paso 3: El Switch Core1 realiza el envío del Ping al Switch FACHSE – Q. (Ver Fig. N° 08)

Fig. N° 08: Enrutamiento del Switch Core1 a la FACHSE – Q.



- Paso 4: El Switch FACHSE – Q realiza el envío del Ping al Host de destino. (Ver Fig. N° 09)

Fig. N° 09: Entre de Ping al Host Final (PC-12).

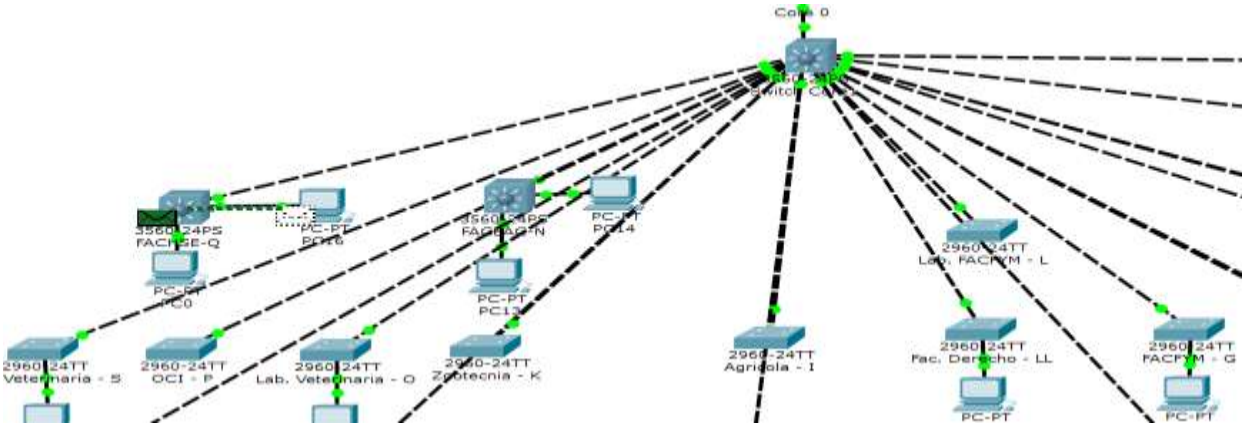


Fig. N° 10: Ping exitoso entre nodos IPv6.

Fire	Last Status	Source	Destination	Type	Color	Time(sec)	Periodic
	Successful	PC2	2001:DB8:39::5	ICMPv6		5.000	Y

CAPÍTULO VIII

CONCLUSIONES Y RECOMENDACIONES

VIII. CONCLUSIONES Y RECOMENDACIONES

8.1. Conclusiones

1. Sí es posible la migración en forma gradual de IPv4 a IPv6 en la red Telemática de la Universidad Nacional Pedro Ruiz Gallo, en este caso usamos el mecanismo de transición Dual Stack para ejecutar la migración gradual.

2. Las ventajas de la migración en forma gradual de IPv4 a IPv6 son claramente visibles como la obtención de mayor cantidad de host, mayor ancho de banda, aumento de seguridad y velocidad.

3. Debido al agotamiento de las direcciones IPv4, es de suma importancia que todas las redes sean migradas lo antes posible al nuevo protocolo IPv6, para aprovechar todavía este tiempo que queda como tiempo de transición para solventar los posibles inconvenientes que puedan darse en la migración total.

4. IPv6 es un paso, más bien evolucionario y no revolucionario de IPv4, dado por la IETF, el cual conserva muchas de las bondades de IPv4, pero a la vez mejora las debilidades de IPv4. IPv6 permite direccionar 2128 nodos, y lo hace con una arquitectura de direcciones simple y fija, lo cual permite una fácil planificación reduciendo así el manejo de las redes.

5. La seguridad que conlleva el migrar a IPv6, es un aumento en la seguridad a nivel de capa de red, pues IPsec se vuelve obligatorio, lo cual permite crear toda una estructura de seguridad más robusta, y da paso a crear aplicaciones más seguras.

6. Windows y Cisco ya tienen el soporte necesario para poder migrar aquellas redes que cuenten con una estructura desarrollada en dichas plataformas, los comandos necesarios para dicha migración ya fueron creados y lo único que se necesita es una buena planificación para posteriormente poner en marcha la migración a IPv6 para poder aprovechar las bondades de este nuevo protocolo.

8.2. Recomendaciones

1. Actualmente un buen porcentaje de redes están todavía trabajando con el protocolo IPv4, y sólo un pequeño porcentaje ya lo comienza a hacer con el nuevo protocolo IPv6. Debido a esto, se considera que éste es un buen momento de experimentación para comenzar a hacer las pruebas de migración hacia el nuevo protocolo IPv6, así como de comenzar a familiarizarse con las características propias de IPv6 y con ello poder realizar una buena planificación de migración.

2. Al estudiar los equipos con que cuenta La red telemática observamos que hay equipos que soportan la IPv6 pero a su vez se necesita la compra de nuevos equipos modernos para poder hacer realidad esta migración gradual.

3. Los tres mecanismos de transición son posibles realizar en la red telemática, sin embargo se acomodaría mejor el mecanismo de transición Dual Stack, debido a como está estructurada la red en la Universidad Nacional Pedro Ruiz Gallo.

CAPÍTULO IX

BIBLIOGRAFÍA - LINKOGRAFÍA Y ANEXOS

IX. BIBLIOGRADIA – LINKOGRAFIA Y ANEXOS

9.1. Bibliografía

- [Blanchet, 2009] Blanchet, M. (2009). Migrating to IPv6: A Practical Guide to Implementing IPv6 in Mobile and Fixed Networks. Wiley.

- [Hagen, 2014] Hagen, S. (2014). IPv6 Essentials. O'Reilly Media.

- [NEWS, 20] NEWS, I. (20). Remaining ipv4 addresses to be redistributed to regional internet registries, address redistribution signals that ipv4 is nearing total exhaustion. info, 1:1_22.

- [Peterson and Davie, 2011] Peterson, L. and Davie, B. (2011). Computer Networks: A Systems Approach. The Morgan Kaufmann Series in Networking. Elsevier Science.

- [Postel, 1981] Postel, J. (1981). Rfc 791: Internet protocol.

- [Tanenbaum and Wetherall, 2011] Tanenbaum, A. and Wetherall, D. (2011). 5ta edition, Computer Networks. Pearson Prentice Hall.

- [van Beijnum, 2005] van Beijnum, I. (2005). Running IPv6. Expert's voice in networking. Apress.

- [Universidad de San Carlos de Guatemala, Migración de IPv4 a IPv6, 2009]

- [Red Telemática de la Universidad Nacional Pedro Ruiz Gallo]

9.2. Linkografía

- http://belarmino.galeon.com - [Universidad privada cumbre, Redes I]

- www.cisco.com – CCNA1, Módulo2

9.3. Anexos

- www.rfc-editor.org
- RFC 791. Internet Protocol. Estados Unidos. 1981.
- RFC 792. Internet Control Message Protocol. 1981.
- RFC 1112. Host extensions for IP multicasting. 1989.
- RFC 1918. Address Allocation for Private Internets. 1996.
- RFC 2401. Security Architecture for the Internet Protocol. 1998.
- RFC 3330. Special-Use IPv4 Addresses. 2002.
- RFC 2460. Internet Protocol, Version 6 (IPv6) Specification. 1998.