



**UNIVERSIDAD NACIONAL AUTÓNOMA  
DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN**

**PROPUESTA DE IMPLEMENTACIÓN DEL PROTOCOLO IPV6  
EN LA RED INALAMBRICA UNIVERSITARIA**

**TESIS PROFESIONAL**

**ARTURO MARTINEZ MORENO.**



MÉXICO, 2012.



Universidad Nacional  
Autónoma de México



**UNAM – Dirección General de Bibliotecas**  
**Tesis Digitales**  
**Restricciones de uso**

**DERECHOS RESERVADOS ©**  
**PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL**

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.



**UNIVERSIDAD NACIONAL AUTÓNOMA  
DE MÉXICO**

**FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN**

**PROPUESTA DE IMPLEMENTACIÓN DEL PROTOCOLO  
IPV6 EN LA RED INALAMBRICA UNIVERSITARIA**

**TESIS PROFESIONAL  
PARA OBTENER EL TITULO DE:  
INGENIERO MECÁNICO ELECTRICISTA**

**PRESENTA:**

**ARTURO MARTÍNEZ MORENO**

**ASESOR:**

**ING. VICTOR RAÚL VELASCO VEGA**



MÉXICO, 2012.

**“Nihil Adeo Arduum Est Qvod Virtute Consequi Non Possit”**

"Nada es tan difícil que no se pueda conseguir con coraje"

Julio Cesar.

## **Agradecimientos**

En primera instancia, quiero agradecer a Dios que, aunque más de una vez he renegado de su existencia, nunca ha dejado de darme muestras de la misma. La muestra está en que el día de hoy estoy a punto de titularme rodeado de las personas que amo y me aman. Gracias Señor por permitirme vivir este momento.

Le agradezco a Dios por haberme dado lo más importante que tengo, que es mi familia. En todo momento de mi existencia nunca me ha dejado solo, me da la fuerza para cumplir mis objetivos y gozar de los frutos con mi familia y mis amigos.

Mi familia por estar a mi lado en todo momento,, apoyándome en las situaciones más difíciles, me ayudaron a levantarme de las adversidades y aprender de los errores. Su apoyo fue y es fundamental. Les agradezco por todo lo que me han brindado.

Al Ing. Víctor Velasco por apoyarme en la realización del presente trabajo. Su apoyo a sido fundamental para concretar este trabajo tan anhelado.

A los compañeros del departamento de redes, al haberme brindado su amistad y su apoyo. Les dos gracias a cada uno. Gracias a su apoyo, el día de hoy puedo enfrentarme a cualquier circunstancia y salir adelante.

Arturo Martínez Moreno.

# Índice.

<b>Tema</b>	<b>... 1</b>
<b>Introducción.</b>	<b>... 2</b>
<b>Síntesis capitular.</b>	<b>... 4</b>
<b>Capítulo1. Fundamentos teóricos de telecomunicaciones.</b>	<b>... 5</b>
1.1.- Modelo de Interconexión de Sistemas Abiertos (OSI)	... 5
1.2.- Ventajas del modelo OSI.	... 6
1.3.- Descripción de las capas del modelo OSI.	... 6
1.4.- Protocolo de Control de Transmisión / Protocolo de Internet (TCP/IP).	...10
1.5.- Descripción de las capas del modelo TCP/IP.	... 10
1.6.- Comparación del modelo OSI contra el protocolo TCP/IP.	... 12
1.7.- Protocolo de Internet versión 4 (IPv4).	... 13
1.8.- Clase de direcciones.	... 16
1.9.- Enrutamiento entre Dominios sin Clase (CIDR).	... 17
1.10.- Mascara de Subred de Longitud Variable (VLSM).	... 17
<b>Capítulo2. Introducción a las redes inalámbricas.</b>	<b>... 18</b>
2.1.- Clasificación de las redes.	... 18
2.2.- Topología de una red.	... 20
2.3.- Redes Inalámbricas.	... 22
2.4.- Elementos de una red inalámbrica.	... 24
2.4.1.- Punto de Acceso o Access Point (AP).	... 24
2.4.2.- Antenas.	... 25
2.4.3.- Tarjeta de Interfaz de Red (NIC).	... 25
2.4.4.- SSID (Service Set Identifier).	... 26
2.5.- Estándar IEEE 802.11 a/b/g/n.	... 26
2.6.- Topología de redes inalámbricas.	... 28
2.6.1.- Topología Ad-hoc.	... 28
2.6.2.- Topología infraestructura.	... 28
2.7.-Acceso Múltiple por Detección de Portadora con detección de colisión ( CSMA/CD).	... 29
2.8.-Acceso Múltiple por Detección de Portadora con evasión de colisión (CSMA/CA).	... 29
2.9.-Mecanismos de seguridad en las redes inalámbricas.	... 30
2.9.1.-Amenazas de seguridad en redes inalámbricas.	... 30
2.9.2.-Mecanismos de seguridad en redes inalámbricas.	... 31
<b>Capítulo3.Red Inalámbrica Universitaria en la UNAM.</b>	<b>... 33</b>
3.1.- Infraestructura.	... 33
3.2.- Switch controlador.	... 38
3.3.- Configuración general del switch controlador.	... 38
3.4.- Esquema de configuración lógica.	... 48

<b>Capitulo4. ProtocoloIPv6.</b>	<b>... 50</b>
4.1.- Introducción al protocolo IPv6.	... 50
4.2.- Cabecera del protocolo IPv6.	... 51
4.3.- Formato del direccionamiento IPv6.	... 52
4.4.- Direccionamiento en IPv6.	... 54
4.4.1.- Unicast.	... 54
4.4.2.- Anycast.	... 57
4.4.3.- Multicast.	... 58
4.5.- Asignación de direcciones IPv6.	... 60
4.5.1.- Manual.	... 60
4.5.2.- Autoconfiguración Stateless.	... 60
4.6.- Direcciones IPv6 reservadas.	... 60
4.7.- Técnicas de transición.	... 61
4.7.1.- DualStack.	... 61
4.7.2.- Tunneling.	... 62
<b>Capitulo5. Propuesta de implementación del protocolo IPv6 en la Red Inalámbrica Universitaria.</b>	<b>... 65</b>
5.1.- Definición de configuración.	... 65
5.2.- Propuesta de configuración física del switch controlador “Master”	... 66
5.3.- Propuesta de configuración lógica del switch controlador “Master”	... 67
5.4.- Configuración del punto de acceso.	... 71
5.5.- Prueba de la configuración.	... 73
5.6.- Propuesta de implementación del protocolo IPv6 en la Red Inalámbrica Universitaria (RIU).	... 75
5.6.1.- Ejemplo de implantación del protocolo IPv6 para la FES-Aragón.	... 81
<b>Capitulo6.Resultados obtenidos.</b>	<b>... 85</b>
6.1.-Resultados.	... 85
6.2.-Comprobación de conexión de red con IPv6.	... 86
<b>Conclusiones</b>	<b>... 89</b>
<b>AnexoA</b>	<b>... 92</b>
<b>AnexoB</b>	<b>... 94</b>
<b>Glosario</b>	<b>... 100</b>
<b>Bibliografía</b>	<b>... 111</b>

## **Tema**

Propuesta de implementación del protocolo IPv6 en la Red Inalámbrica Universitaria.

## **Problemática**

¿Está preparada la Red Inalámbrica Universitaria (RIU) para implementar el protocolo de Internet versión 6 (IPv6)?

## **Hipótesis.**

Debido al crecimiento de dispositivos móviles que utilizan el Protocolo de Internet versión 4 (IPv4) como medio de comunicación y transmisión de datos (Smartphones, laptops, tablets, por mencionar algunos), el direccionamiento del protocolo IP en la versión 4, resultara insuficiente en poco tiempo. Debido a esto, la implementación del protocolo IPv6 en la infraestructura de la Red Inalámbrica Universitaria (RIU), asegurará su crecimiento para los próximos años, ya que el nuevo protocolo ofrece un direccionamiento superior al usado por el protocolo IPv4.

## **Objetivo general.**

Llevar a cabo una serie de pruebas con el protocolo de Internet versión 6 (IPv6) en la infraestructura de la Red Inalámbrica Universitaria (RIU). Dichas pruebas tendrán como finalidad la implementación del protocolo IPv6 de forma nativa. De igual forma, este protocolo deberá trabajar en forma conjunta y estable con el actual protocolo de Internet versión 4 (IPv4). Además, la implementación propuesta deberá ofrecer el mismo servicio estable y confiable como el que se brinda hasta el momento en la RIU.

## **Objetivo específico:**

Llevar a cabo las pruebas de configuración en el Switch controlador y el Sistema Operativo que se determinaron, con la finalidad de determinar los elementos necesarios para llevar a cabo la materialización de la implantación del protocolo IPv6 en la infraestructura actual de la Red Inalámbrica Universitaria.



## Introducción.

La Universidad Nacional Autónoma de México, en su quehacer diario, está en la búsqueda de conocimiento para beneficio de la comunidad universitaria y de la sociedad mexicana, convirtiéndola de esta forma en nuestra máxima casa de estudio.

En la década de 1970, los creadores de Internet crearon un protocolo el cual permite establecer la comunicación entre dos dispositivos o host a través de una red. El cual consiste en configurar en cada dispositivo una dirección lógica llamada dirección IP. Para comprender mejor este concepto podemos hacer una analogía con el correo postal, la dirección IP representa la dirección de nuestro domicilio, la cual, cuenta con un número, calle, código postal y colonia. Estos datos deben ser únicos para identificar y localizar nuestra posición. Este hecho permite encontrar un dispositivo en la red e interactuar con este.

Los desarrolladores de Internet nunca imaginaron que los 24 mil millones de direcciones IP se agotarían. Pero el día 12 de febrero de 2011, la Autoridad de Asignación de Números de Internet IANA (por sus siglas en inglés, Internet Assigned Numbers Authority) entregó los últimos bloques de direcciones disponibles.

*03 de Febrero de 2011<sup>1</sup>*

*Montevideo, febrero 2011.- El Registro de Direcciones de Internet de América Latina y el Caribe, LACNIC, comunica que el stock central de direcciones IPv4 administrado por la IANA (Internet Assigned Numbers Authority) ha quedado finalmente agotado, lo que desencadena el irreversible proceso de cambio de protocolo de Internet. De acuerdo a la política global acordada por la comunidad de Internet en todas las regiones, hoy fueron entregados los últimos bloques disponibles de direcciones IPv4 correspondiendo uno para cada uno de los cinco Registros Regionales de Internet (RIR) en todo el mundo.*

*"Este es un día histórico en la vida de Internet, y que hemos estado*

*Esperando desde hace bastante tiempo", afirmó Raúl Echeverría, Director ejecutivo de LACNIC. "El futuro de Internet está en IPv6. Se terminaron las direcciones IPv4 del stock central de ICANN y desde ahora deberemos manejarnos únicamente con el stock que LACNIC cuenta", agregó.*

Con la entrega de los últimos bloques de direccionamiento IPv4, simbólicamente se terminaron las direcciones IP para ser entregados por la IANA a los Registros Regionales de Internet o RIR (por sus siglas en inglés, Regional Internet Registry). Aunque, estos últimos aun conservan bloques de direcciones para ser entregados a sus

---

<sup>1</sup> <http://www.lacnic.net/sp/anuncios/2011-agotamiento-ipv4.html>

respectivos ISP regionales. Por lo que se estima que para el año 2015 se agoten realmente las direcciones.

Este suceso se veía lejos o más aun, inalcanzable para los creadores de Internet. Aunque este suceso ya era esperado, desde inicios de la década de 1990 se comenzó a trabajar en el diseño del un nuevo protocolo para Internet, la versión del protocolo para Internet 6 o IPv6.

En el año de 1998, la UNAM inicio con las investigaciones en IPv6 y posteriormente realizando las primeras pruebas reales en este tema. En los años siguientes la UNAM creo la primera red en IPv6 en México, con lo cual, se iniciaron las primeras pruebas reales en sistemas de telecomunicaciones y en aplicaciones.

En el presente trabajo, se discutirá los diferentes problemas que conlleva implementar el protocolo IPv6 en la RIU, la cual, su infraestructura está basada en el protocolo de Internet versión 4 o IPv4.

Hay varios motivos para implementar el protocolo IPv6 en la RIU, el principal, es asegurar el crecimiento de la RIU. Ya que, en los últimos años, el número de usuarios ha crecido de forma considerable. Un factor, ha sido la adquisición de teléfonos celulares y notebooks con tarjetas inalámbricas.

Además la utilización de IPv6 en la RIU, proporcionaría un mayor rango de direcciones validas, la cuales, permitirá ofrecer nuevos servicios a los usuarios de la RIU. Actualmente en la RIU se usan direcciones privadas o no homologadas, este tipo de direcciones no son validas para ser usadas en Internet. Para solucionar este problema, se hace el uso de un mecanismo que traduce las direcciones no validas de los usuarios por un traductor o un Traductor de Direcciones de Red o NAT (por sus siglas en inglés, Network Address Translation). Con la implementación del protocolo IPv6 ya no será necesario hacer uso de este mecanismo, ya que, todas las direcciones IPv6 son validas.

El primer gran beneficio que ofrece IPv6 en contra de IPv4, es la gran cantidad de direcciones disponibles. En IPv4 se usan 32 bits para formar las direcciones IP y en IPv6 en cambio, usa 128 bits, con lo cual otorga  $5 \times 10^{28}$  de direcciones IP, se prevé que a cada habitante del planeta se le asignara 10 direcciones IPv6. Esta gran cantidad de direcciones nos permitiría crecer sin preocupaciones.

Cabe hacer mención, que la implementación del protocolo IPv6 está en su fase de pruebas, lo cual quiere decir, que ya ha pasado la fase de investigación. Varias organizaciones (Google, Microsoft, Yahoo!, Telefónica y otros) han realizado pruebas para implementar este protocolo y estudiar las opciones de acuerdo a sus necesidades. En el presente trabajo se verán cuáles son las posibilidades y los requerimientos necesarios para implementar IPv6 en la RIU.

## **Síntesis capitular.**

### **Capítulo 1. Fundamentos teóricos de telecomunicaciones.**

Capítulo dedicado al modelo de referencia OSI y de los protocolo TCP e IP, también conocidos como Protocolo de Control de Transmisión/ Protocolo de Internet (TCP/IP).

### **Capítulo 2. Introducción a las redes inalámbricas.**

Capítulo dedicado a la clasificación de las redes inalámbricas, así como a la descripción de los elementos que conforman una red inalámbrica.

### **Capítulo 3. Red Inalámbrica Universitaria en la UNAM.**

Capítulo dedicado a la descripción de la infraestructura actual de la Red Inalámbrica Universitaria (RIU), así como de la configuración física y lógica del Switch Controlador Aruba.

### **Capítulo 4. Protocolo IPv6.**

Capítulo dedicado a la descripción del protocolo de Internet versión 6

### **Capítulo 5. Propuesta de implementación del protocolo IPv6 en la Red Inalámbrica Universitaria**

Capítulo dedicado a la propuesta de configuración tanto física como lógica de cada unos de los elementos que conforman la red.

### **Capítulo 6. Resultados obtenidos.**

Capítulo dedicado a la reseña de los resultados obtenidos de la configuración física y lógica propuesta.

### **Conclusiones.**

Apartado dedicado a las conclusiones obtenidas de la prueba realizada.

### **Anexos**

Contiene algunas referencias complementarias del presente trabajo.

### **Bibliografía.**

Material utilizado y consultado para la elaboración del presente trabajo.

### **Glosario.**

Referencias realizadas al significado de conceptos utilizados en este trabajo.

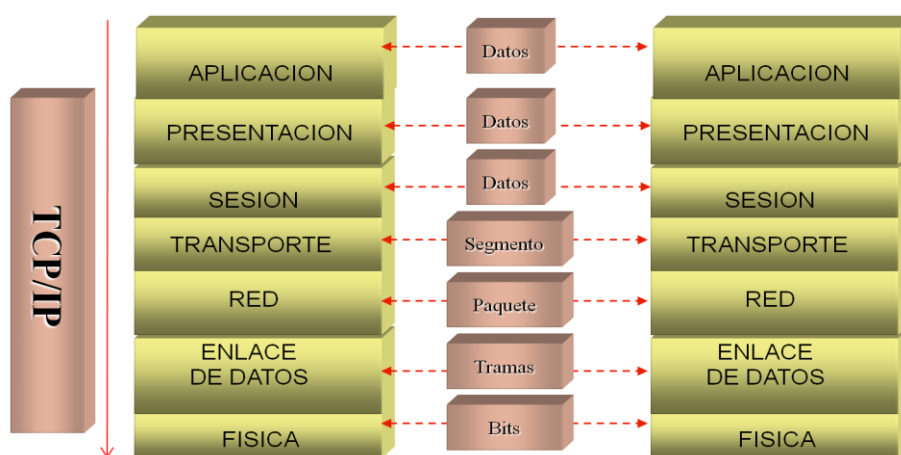
# Capítulo 1. Fundamentos teóricos de telecomunicaciones.

A medida que las redes ganaban terreno en las áreas de educación, industria y medicina, etc., las organizaciones que requerían expandir su red solo tenían la opción de adquirir equipos con su actual proveedor, debido a la utilización de protocolos “Proprietarios” o “Cerrados”. La utilización de protocolos “Proprietarios” impedía que redes de diferentes fabricantes pudieran establecer una comunicación. Tal situación dio paso a que la Organización Internacional de Normalización o ISO (por sus siglas en inglés, International Organization for Standardization) desarrollara el modelo de Interconexión de Sistemas Abiertos (por sus siglas en inglés, Open System Interconnection), conocido como modelo OSI.

## 1.1.- Modelo de Interconexión de Sistemas Abiertos (OSI).

El modelo OSI conocido como un modelo de referencia, ya que proporciona un conjunto de lineamientos que busca la manera de asegurar una mayor compatibilidad e interoperabilidad entre los equipos de distintos fabricante.

El modelo OSI ofrece una visión del tratamiento que se le da a los datos durante la comunicación host a host. Los datos pasan por una serie de capas, donde cada capa, le añade un encabezado con información adicional (encapsulación). Este encabezado indica como debe ser tratada la información del lado del receptor al momento de establecer la comunicación.



Cuadro 1. Encapsulación de la información.

## 1.2.- Ventajas del modelo OSI.

- Reduce la complejidad.
- Estandariza las interfaces.
- Facilita la ingeniería modular.
- Asegura la interoperabilidad.
- Simplifica la enseñanza y el aprendizaje.

## 1.3.- Descripción de las capas del modelo OSI.

El manejo del modelo OSI en capas, proporciona una visión esquemática del tratamiento o encapsulación que se le da a la información en cada una de las capas.

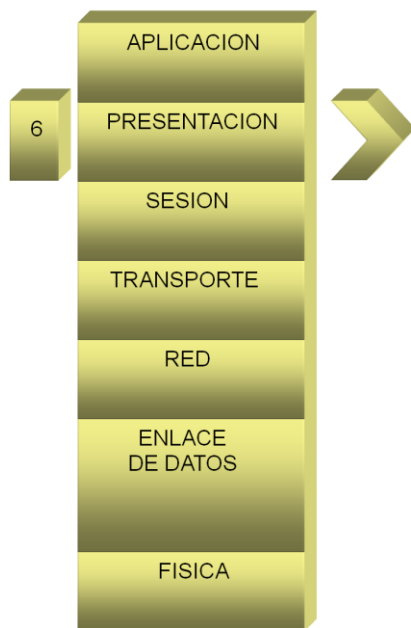
### Capa 7. Aplicación (Servicio de red a aplicaciones).



- Es la capa mas cercana al usuario.
- Proporciona servicios de red a los procesos de aplicaciones (ejemplo, correo electrónico, transferencia de archivos y emulación de terminales).
- Proporciona la interfaz del usuario con las aplicaciones.
- Controla la integridad de los datos.
- Algunos de los protocolos que pertenece a la capa de aplicación son: DNS, FTP, HTTP, SMTP, SQL, IMAP y POP3

Cuadro 2. Capa de aplicación.

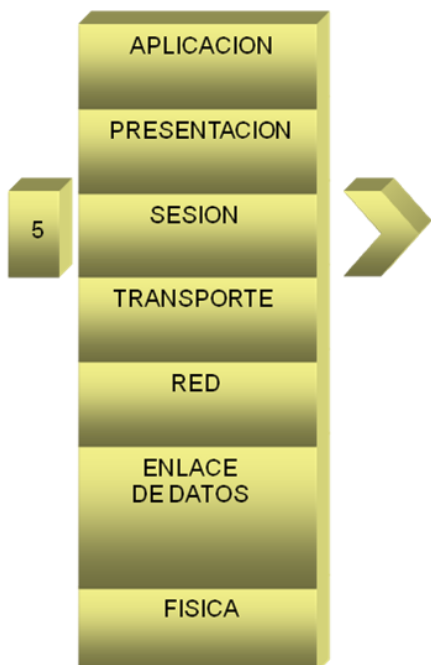
### Capa 6. Presentación (Representación de los datos).



- Es la capa encargada de garantizar que los datos sean legibles para el sistema receptor.
- Es la capa donde se le da formato o estructura a los datos: compresión, encriptación y decodificación.
- Negocia que el sistema transfiera los datos a la capa de aplicación.
- Algunos de los protocolos que pertenece a la capa de presentación son: ASCII, JPEG, DOC, GIF, etc.

Cuadro 3. Capa de presentación.

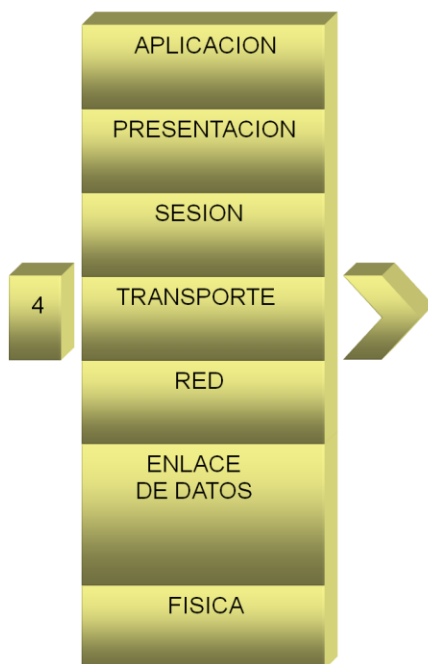
### Capa 5. Sesión (Comunicación entre dispositivos de la red).



- Es la capa que administra inicia y termina la sesión entre aplicaciones.
- Sincroniza el dialogo entre capas e intercambio de datos.
- Presta servicio a la capa de presentación.
- Reinicia sesiones interrumpidas o inactivas durante un largo periodo de tiempo
- Algunos de los protocolos que pertenece a la capa de red son: RPC, LDAP y servicio de sesión NetBIOS.

Cuadro 4. Capa de sesión.

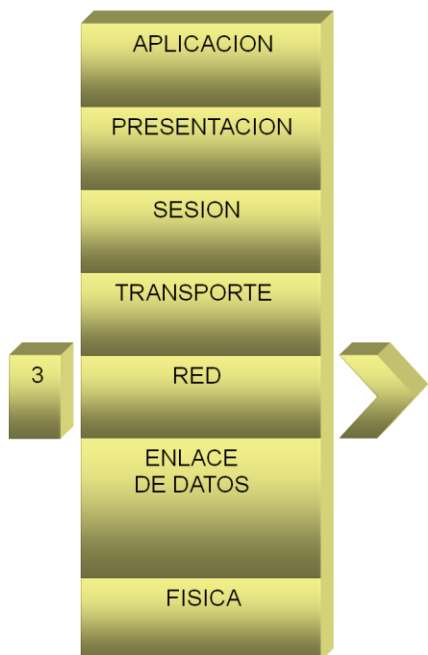
#### Capa 4. Transporte (Conexión extremo a extremo y fiabilidad de los datos).



- Es la capa encargada de establecer, mantener, terminar circuitos virtuales.
- Asegura la fiabilidad de los datos y el flujo de control.
- Proporciona la comunicación entre distintos programas de aplicación.
- Detección de fallas y control del flujo de información de recuperación.
- Algunos de los protocolos que pertenecen a la capa de transporte son: UDP, TCP y SPX

Cuadro 5. Capa de transporte.

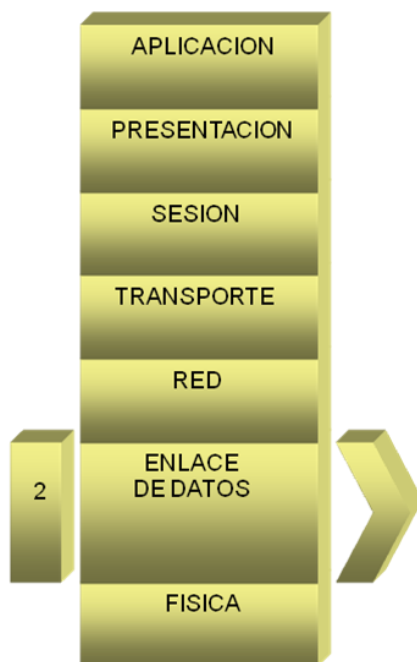
#### Capa 3. Red (Direccionamiento lógico).



- Es la capa responsable de seleccionar la mejor ruta para llegar a un destino.
- Define el direccionamiento lógico.
- Provee transferencia confiable de datos a través de los medios.
- Algunos de los protocolos que pertenecen a la capa de red son: IP, IPX y AppleTalk

Cuadro 6. Capa de red.

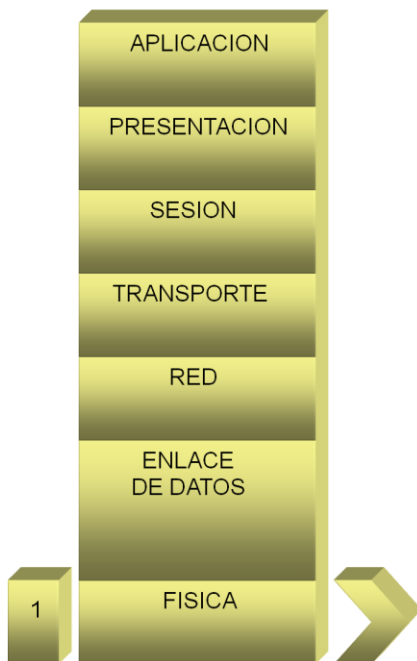
## Capa 2. Enlace de datos (Direccionamiento físico).



- En esta capa se define el direccionamiento físico.
- Provee transferencia confiable de datos a través de los medios.
- Proporciona la detección de errores a través de los FCS (Errores de secuencia cíclica).
- Define como los datos son formateados para su transmisión y como acceder al medio.
- Algunos de los protocolos que pertenece a la capa de enlace son: LAPB, LAPD y LLC.

Cuadro 7. Capa de enlace de datos.

## Capa 1. Física (Señal y transmisión binaria).



- Esta capa define las características y funciones de los elementos que interactúan en la red: cables, conectores, voltajes y distancias máximas de transmisión.
- Es la capa responsable de convertir los bits o bytes de acuerdo al medio seleccionado (pulsos eléctricos o señales luminosas).
- Algunos de los protocolos que pertenece a la capa de aplicación son: EIA/TIA 568 A y B, RS232, 10BaseT, 10 Base 2, 10 Base 5 y USB.

Cuadro 8. Capa física.



#### 1.4.- Protocolo de Control de Transmisión/Protocolo de Internet (TCP/IP).

El modelo TCP/IP es también conocido como modelo de protocolo, ya que a diferencia del modelo OSI, este debe seguirse estrictamente para asegurar la comunicación. Este modelo fue creado en la década de 1970 por DARPA.

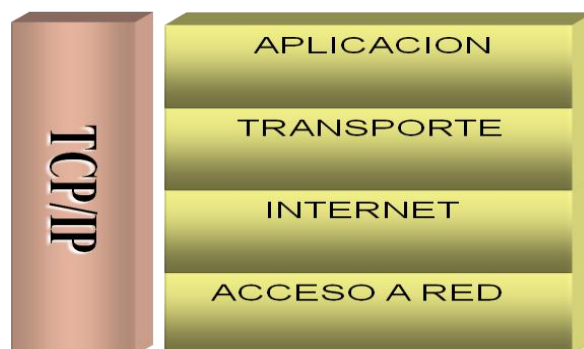
El modelo TCP/IP de igual forma que el modelo OSI, es un estándar abierto. Esto significa que cualquiera puede usar el modelo TCP/IP. Este modelo fue desarrollado por el Departamento de Defensa de los Estados Unidos con el objetivo de diseñar un protocolo que permitiera transmitir sin importar el medio (cable Ethernet, cable coaxial o fibra óptica).

#### 1.5.- Descripción de las capas del modelo TCP.

TCP/IP está compuesto por dos suites de protocolo, Protocolo de Control de Transmisión o TCP (Transmission Control Protocol) y del Protocolo de Internet o IP (Internet Protocol). TCP/IP está dividido en cuatro capas y cada una resuelve una tarea relacionada con la transmisión de los datos.

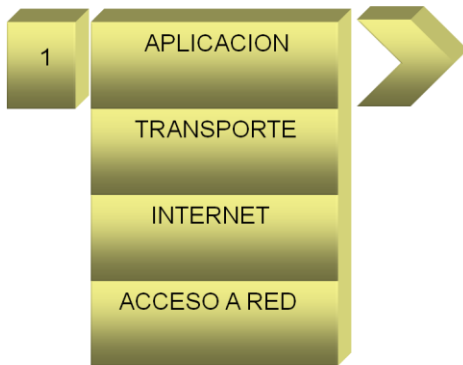
El modelo TCP/IP está dividido en las siguientes capas:

- Capa de aplicación.
- Capa de transporte.
- Capa de internet.
- Capa de acceso a la red.



Cuadro 9. Modelo TCP/IP.

### Capa 1. Aplicación.

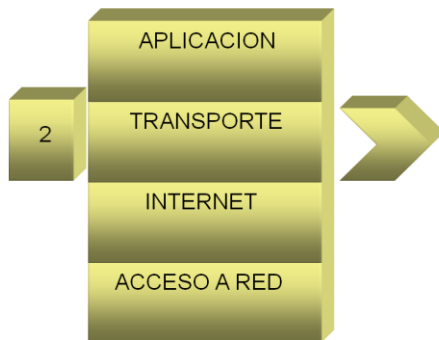


- Capa de Aplicación. Comprende las funciones de las capas de aplicación, presentación y sesión del modelo OSI.

- Representa los datos de aplicación que se presentan al usuario. Por ejemplo,, HTTP presenta datos al usuario en un navegador web, por ejemplo, Internet Explorer.

Cuadro 10. Capa de aplicación.

### Capa 2. Capa de Transporte.

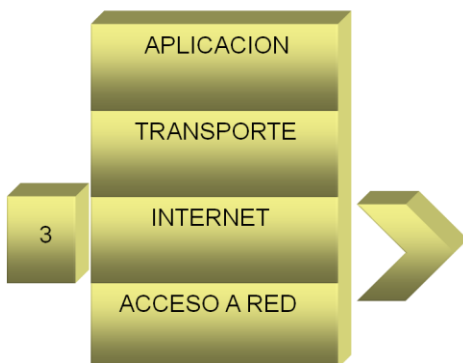


- Capa de Transporte. Esta capa tiene las funciones de la capa de transporte del modelo OSI.

- Soporta la comunicación entre dispositivos y realiza la corrección de errores

Cuadro 11. Capa de transporte.

### Capa 3. Internet.

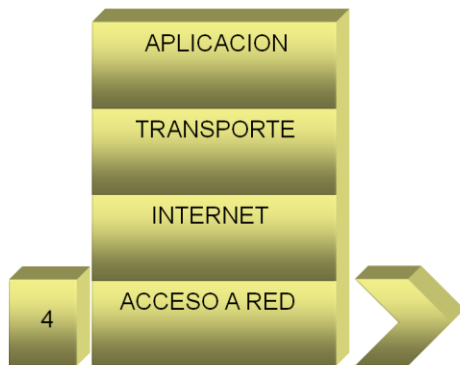


- Capa de Internet. Capa equivalente a la capa de Red del modelo OSI.

- La capa de red selecciona la mejor ruta a través de la red para entregar la información.

Cuadro 12. Capa de Internet.

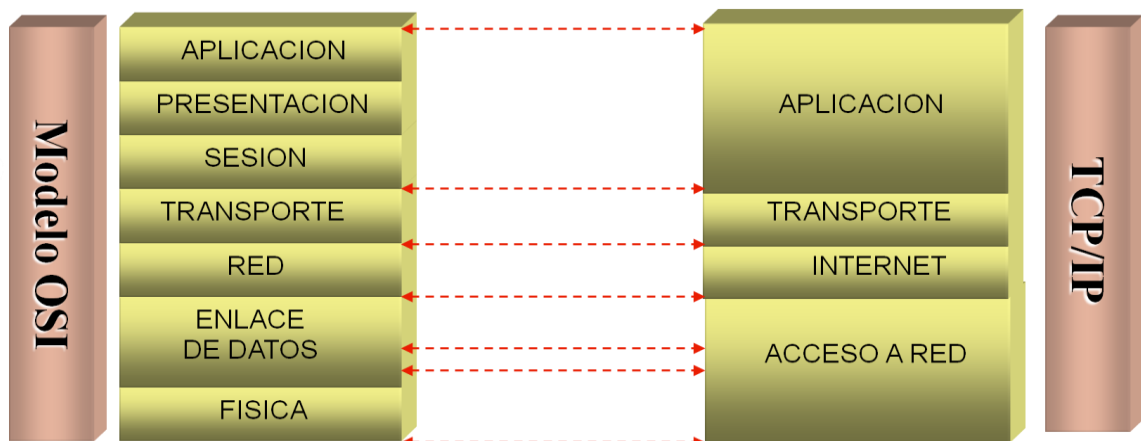
### Capa 1. Acceso a Red



- Capa de Acceso a red. Comprende las capas de Enlace de datos y Física del modelo OSI.
- La capa de enlace le da formato a los datos para su transmisión y el acceso a la red.
- La capa física define los aspectos eléctricos y mecánicos

Cuadro 13. Capa de acceso a red.

### 1.6.- Comparación del modelo OSI contra el protocolo TCP/IP.



Cuadro 14. Relación que guardan entre si el modelo OSI y el modelo TCP/IP.

Similitudes entre los modelos OSI y TCP/IP:

- Ambos se dividen en capas.
- Ambos tienen capas de aplicación, aunque incluyen servicios muy distintos.
- Ambos tienen capas de transporte y de red similares.
- Se supone que la tecnología es de conmutación por paquetes y no de conmutación por circuito.
- Los profesionales de networking deben conocer ambos modelos.

Diferencias entre los modelos OSI y TCP/IP:

- TCP/IP combina las capas de presentación y de sesión en una capa de aplicación
- TCP/IP combina la capas de enlace de datos y la capa física del modelo OSI en una sola capa
- TCP/IP parece ser más simple porque tiene menos capas

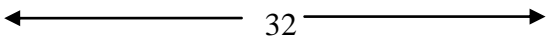
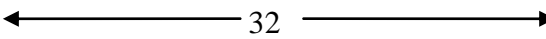
### 1.7.- Protocolo de Internet versión 4 (IPv4).

La comunicación entre dispositivos en Internet está basada en la utilización del direccionamiento IPv4. Esto quiere decir que, cada dispositivo debe ser configurado con una dirección IPv4, que puede ser asignada de forma manual o de forma automática.

Una dirección IP es un identificador numérico, de carácter lógico y jerárquico, que, identifica a la interfaz de un equipo de cómputo en la red.

Una dirección IPv4 está conformada por cuatro octetos delimitados o separados por puntos ( . ). La suma de los cuatro octetos nos da el total de 32 bits. Las direcciones IPv4 se pueden representar en formato decimal para una mejor compresión, de igual forma que en la notación binaria, estas son separadas por puntos.

Como ejemplo, se muestra una dirección IPv4 en notación binaria y decimal.

Notación	IPv4
Binario	11000000.10101000.00000001.00000001 
Decimal	192.168.1.1
Binario	10000100.11111000.01111000.00111011 
Decimal	132.248.120.59

**Tabla 1. Ejemplo de dirección es IPv4 en notación binaria y decimal.**

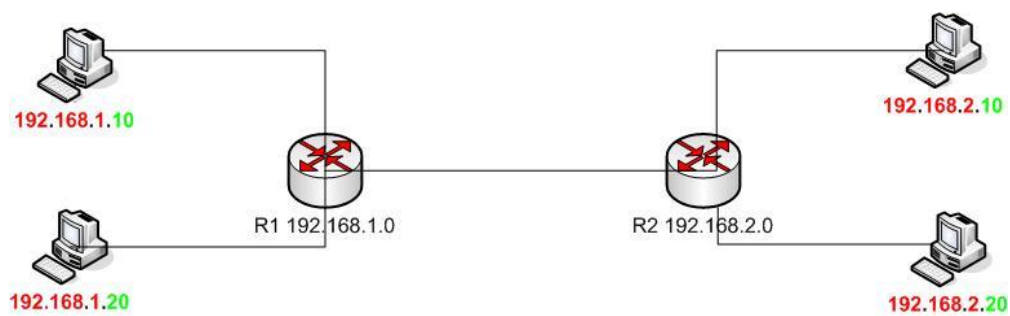
Como se puede observar, las direcciones en notación decimal son más sencillas de manejar que las direcciones en notación binaria. No hay que olvidar que los dispositivos utilizan la notación binaria.

Las direcciones IP's constan de dos partes: la parte de red (Network ID) y la parte de host (host ID).

	Network ID	Host ID
Decimal	192.168.1	10
Binario	11000000.10101000.00000001	00001010

**Tabla 2. Conformación de una dirección IP: Network ID y de Host ID**

La porción de red (Network ID), la identifica entre otras redes, mientras que, la porción de host (host ID) identifica individualmente la posición del host en la red.



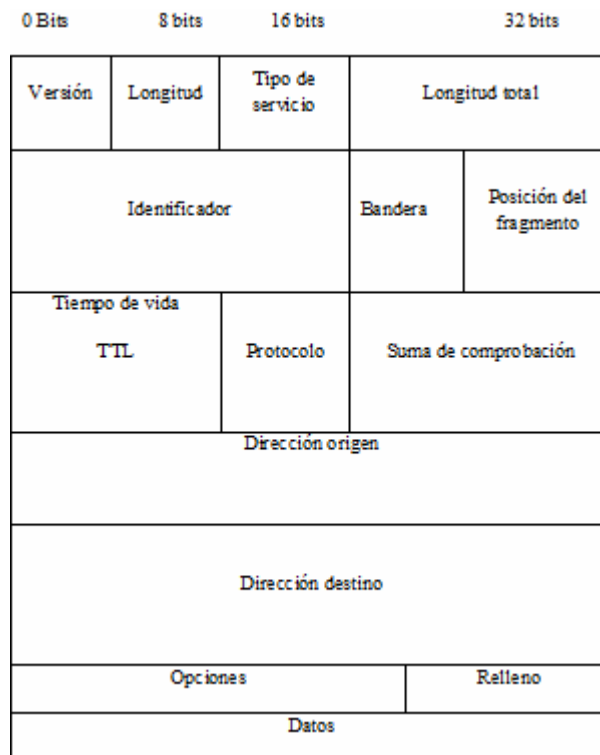
**Diagrama 1. Red 192.168.1.0 y la red 192.168.2.0**

En el diagrama 1, se puede ver de mejor manera el uso de la porción de red y la de host. En color rojo se identifica la porción de red y donde se puede observar que hay dos redes: la 192.168.1.0 y la 192.168.2.0 con dos host por red. Los últimos octetos en color verde identifica la porción de host, la cual identifica la posición del host en la red.

Además de una dirección de red, los equipos deben de contar con una máscara de red y una pasarela o gateway. Con estos tres elementos, cualquier equipo puede establecer una comunicación con otros dispositivos sin importar la red.

Los enrutadores o routers, son los equipos de telecomunicaciones que operan en la capa 3 del modelo OSI, dichos equipos son los encargados de establecer la comunicación entre redes distintas, para ello se valen de la porción de red, la cual es anunciada en su tabla de ruteo.

## Cabecera IPv4.



Cuadro 15. Cabecera del formato TCP/IP.

## Campos de la cabera TCP.

- Versión: Identifica la versión del paquete
- Longitud: Longitud de la cabecera
- Tipo de servicio: Indica una serie de servicios que son deseados durante el Transito del paquete en la red.
- Longitud total: Indica el tamaño total del datagrama en octetos
- Identificador: Indicador único del datagrama.
- Bandera: Indica valores relativos a la fragmentación del paquete.
- Posición del fragmento: Indica la posición de los paquetes fragmentados.
- Tiempo de vida: Indica el número máximo de saltos que un paquete puede pasar De un router a otro.
- Protocolo: Indica el protocolo de las capas superiores al que debe de entregarse El paquete.
- Suma de comprobación: Se recalcula cada vez que un nodo cambia algunos de Sus campos.
- Dirección origen: Indica la dirección IP de quien envía la información.
- Dirección destino: Indica la dirección destino IP, a quien va dirigida la información.
- Opciones
- Datos: Información útil.

### 1.8.- Clase de direcciones.

La organización encargada de la administración de direcciones es la Autoridad para la Asignación de Números de Internet o IANA (por sus siglas en inglés, Internet Assigned Numbers Authority), la cual en un principio determinó el tamaño de las redes. Por lo que las redes las podemos dividir en clases.

Clase	Rango	Total de redes	Total de host
A	1.0.0.0 126.255.255.255	126	16.7 millones
B	128.0.0.0 191.255.255.255	16,384	65,534
C	192.0.0.0 223.255.255.255	2,000,000	254

Tabla 3. Características de las clases de red.

La tabla 2 muestra la clasificación de las redes de acuerdo al tamaño de estas, este tipo de clasificación es también conocida como direccionamiento con Clase o Classful. El direccionamiento con clase fue definido a principios de la década de 1980, en aquel entonces no existía el uso de máscara de red para especificar la porción de red y de host de las direcciones. La forma de hacer la distinción del tamaño de la red fue creando rangos de direcciones.

#### Direcciones especiales:

Tipo	Bloque	Rango	Referencia
Multicast	224.0.0.0/24	224.0.0.0 239.255.255.255	- RFC 1700
Dirección de red	-----	-----	Una por red
Dirección de broadcast	-----	-----	Una por red mas 255.255.255.255
Direcciones experimentales	240.0.0.0	240.0.0.0 255.255.255.255	- RFC 3330
Direcciones del espacio privado	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	10.0.0.0 10.255.255.255 172.16.0.0 172.16.255.255 192.168.0.0- 192.168.255.255	- - RFC 1918
Ruta predeterminada	0.0.0.0/8	0.0.0.0 255.255.255.255	- RFC 1700

Loopback	127.0.0.0/8	127.0.0.0 127.255.255.255	–	RFC 1700
Dirección de enlace local	169.254.0.0	169.254.0.0 169.254.254.254		RFC 3927
Direcciones de test-net	192.0.2.0/24	192.0.2.0 – 192.0.0.255	-----	

Tabla 4. Principales direcciones IP.

El direccionamiento con clase tiene la característica de desperdiciar direcciones de host, ya que, los tamaños de las redes son fijos. A finales de la década de 1980 y a principios de la década de 1990 se introdujo el uso de la máscara de red. La cual permite variar el tamaño de la red de acuerdo a nuestros propósitos.

### 1.9.- Enrutamiento entre Dominios sin Clase (CIDR).

El continuo crecimiento de las redes planteó el problema del agotamiento de las direcciones IPv4. Mientras se diseñaba un nuevo método o la definición de un nuevo estándar para superar el inminente agotamiento de direcciones IPv4, se creó el Enrutamiento de Inter dominios Sin Clase o CIDR (por sus siglas en ingles, Classless Inter Domain Routing).

### 1.10.- Mascara de Subred de Longitud Variable (VLSM).

La Máscara de Longitud Variable o VLSM (por sus siglas en ingles, Variable Length Subnet Mask), hace posible crear subredes, esta técnica, permite un mejor aprovechamiento y mejora la administración de direcciones IP de acuerdo a las necesidades requeridas.

“Las subredes se crean asignando una o más de los bits de host como bits de red. Esto se hace extendiendo el prefijo para “pedir prestado” algunos de los bits de la porción de host de la dirección, a fin de crear bits de red adicionales. Cuantos más bits de host se pidan prestados, mas subredes se pueden definir. Para cada bit prestado, se dobla el número de subredes disponibles. Por ejemplo, si pide prestados 2 bits, puede definir cuatro subredes.

Sin embargo, cada bit prestado, tiene menos bits de host para definir las direcciones de host en cada subred. Por consiguiente, hay menos direcciones de host disponibles por subred. Además, como tiene dos direcciones para cada red (dirección de red y dirección de broadcast) que no se pueden asignar a los host, se reduce el número total de host en la red completa.”<sup>2</sup>

<sup>2</sup> Aspectos básicos de networking Guía de estudio de CCNA, Mark A. Dye, Rick McDonald y Antoon W. Ruffi. Página 247



## Capítulo 2. Introducción a las redes inalámbricas.

Para entender mejor el tema de las redes inalámbricas, primero se debe conocer los tipos de redes que existen. Iniciaremos con la definición de lo que es una red, y posteriormente se describirán las redes inalámbricas de área local o WLAN (Wireless Local Area Network). Ya que este tipo de red es como está configurada la RIU.

*“Del latín rete, el termino red se utiliza para definir a una estructura que cuenta con un patrón característico. Existen múltiples tipos de red, como la red informática, la red eléctrica y la red social. La red informática nombra al conjunto de computadoras y otros equipos interconectados que comparten información, recursos y servicios”.*<sup>3</sup>

La importancia de las redes radica en compartir la información con los demás miembros de una red. También gracias a las redes se comparten recursos, tales como impresoras o escáner, pero, lo que realmente importa es la disponibilidad de la información, y la red ayuda a conseguir este objetivo. Con lo cual aumenta la productividad en los centros de trabajo, ya sea, una escuela, hospital, empresa u hogar.

### 2.1.- Clasificación de las redes.

Las redes se clasifican de acuerdo a su extensión geográfica, su topología, protocolo o por el medio. Nuestra tesis se basa en la propuesta de implementar el protocolo IPv6 en la RIU, la cual es una red inalámbrica del tipo Wireless LAN o WLAN, más adelante se verán las definiciones de las redes WLAN.

Hay que tomar en consideración, que para implementar una red inalámbrica, esta usa la infraestructura de la red cableada, la cual, transporta el tráfico generado por los clientes inalámbricos a un destino.

Para propósitos del presente trabajo, se definen las redes cableadas de acuerdo a su extensión geográfica. El siguiente cuadro sinóptico muestra la clasificación y las características generales de las redes cableadas.

---

<sup>3</sup> <http://definicion.de/red/>

- Red de Área Local (LAN – Local Área Network): Es una red cuyos componentes se encuentran dentro de un área limitada, por ejemplo un edificio o un campus universitario.
- Red de Área Metropolitana (MAN – Metropolitan Area Network): Es una red que se extiende por varios edificios dentro de una misma ciudad. Poseen un cableado especial de alta velocidad para conectarlas utilizando la red de telefonía actual.
- Redes de Área Extensa (WAN – Wide Área Network): Cuando se habla de una red de área extensa se está haciendo referencia a una red que abarca diferentes ciudades e incluso diferentes países.

**Cuadro sinóptico 1. Clasificación de redes cableadas.**

Las redes inalámbricas con el tiempo han ido evolucionando y cumpliendo nuevas funciones, estas redes iniciaron como una extensión de la red LAN. Las cuales, también se pueden dividir por su extensión geográfica. El siguiente cuadro sinóptico muestra la clasificación y las características generales de las redes inalámbricas.

- Red Inalámbrica de Área Personal (WPAN – Wireless Personal Area Network): Incluye redes inalámbricas de corto alcance que abarca un área de algunas decenas de metros. En este tipo de redes generalmente se usa para conectar dispositivos periféricos tales como impresoras, PDA y teléfonos
- Red Inalámbrica de Área Local (WLAN – Wireless Local Area Network): Una WLAN es un tipo de red de área local o (LAN) que utiliza la tecnología de radiofrecuencia en lugar de cables para establecer la comunicación. Esta red sigue el estándar 802.11 con sus diferentes opciones.
- Redes de Área Extensa (WAN – Wide Area Network): Cuando se habla de una red de área extensa se está haciendo referencia a una red que abarca diferentes ciudades e incluso diferentes países.

**Cuadro sinóptico 2. Clasificación de redes inalámbricas.**

Las redes WLAN facilitan en primer lugar, extender la red a lugares donde es difícil o costosa la implementación de una red cableada. De esta forma se logra extender la red LAN con un menor costo, además de agregar nuevos servicios para los usuarios, como sería el caso de implementar VoIP en la red inalámbrica.

## 2.2.- Topología de una red.

La topología de una red es el arreglo físico o lógico, en la cual, los dispositivos se interconectan entre sí para intercambiar información. De las cuales, se pueden dividir principalmente en dos categorías:

Topología lógica: Se refiere a la trayectoria lógica de la señal que pasa por los nodos de la red.

Topología física: Se refiere a la ubicación física de los dispositivos para conformar la red.

Los diferentes tipos de topologías físicas son:

- Topología de bus
- Topología de estrella
- Topología de anillo
- Topología de malla

**Topología de bus.-** En esta topología, todos los dispositivos están conectados en la misma línea de transmisión mediante un cable. La palabra “bus” hace referencia a la línea física que une a todos los dispositivos en la red.

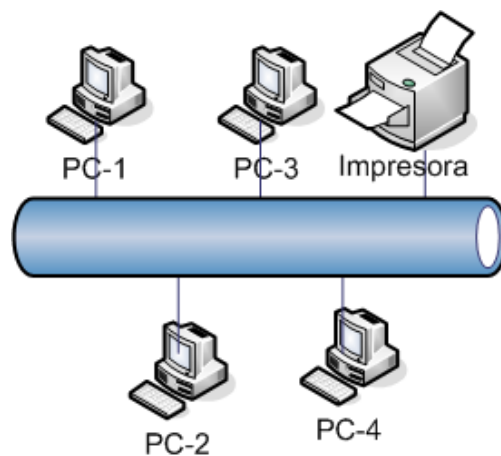


Diagrama 2. Topología de red en bus.

**Topología de estrella.-** En esta topología, los dispositivos están conectados a un equipo central, conocido comúnmente como concentrador o Hub.

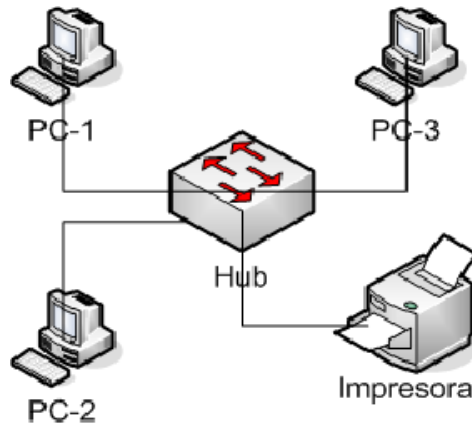


Diagrama 3. Topología de red en estrella.

**Topología de anillo.-** En esta topología, los dispositivos se comunican en turnos y se crea un bucle de equipos en el cual cada uno “tiene su turno para hablar” después del otro.

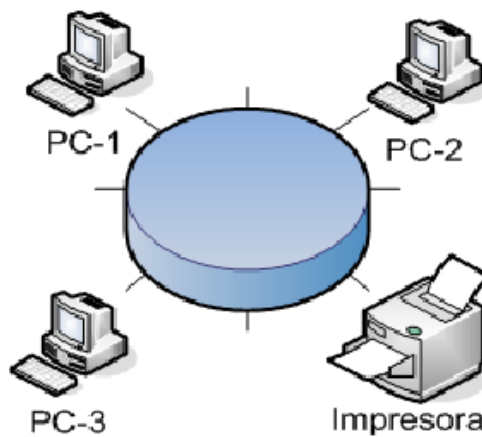


Diagrama 4. Topología de red en anillo.

**Topología de malla.-** En esta topología, todos dispositivos están conectados con todos, estas redes ofrecen una alta tolerancia a fallos gracias a la redundancia que ofrece.

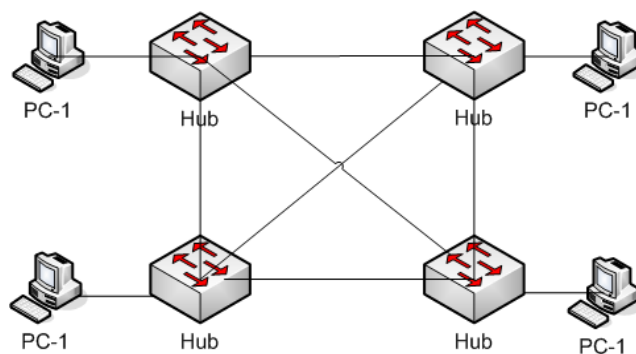


Diagrama 5. Topología de red en malla.

### 2.3.- Redes Inalámbricas.

Como se había comentado, el presente trabajo se basa en las redes inalámbricas de área local o WLAN. Ya que este es el tipo de red inalámbrica a la que pertenece la RIU.

Para iniciar con el tema de redes inalámbricas es importante entender el significado de Wi-Fi y wireless, ya que el primer acrónimo se puede encontrar en diferentes lugares (hoteles, restaurantes, oficinas y centros comerciales etc.), el cual indica que hay un punto de acceso ofreciendo los servicios de red inalámbrica. Mientras que wireless hace referencia a los sistemas de comunicación que usan la modulación de ondas electromagnéticas a través del espacio.

Wi-Fi, es una marca de la Wi-Fi Alliance (anteriormente la WECA: “En pocas palabras, Wi-Fi es la conectividad. En casa, Wi-Fi que se conecta a su contenido favorito y comunicaciones a través de su teléfono móvil, ordenador, reproductores multimedia y Otros dispositivos - todo ello sin cables engorrosos. Cuando usted está en movimiento, Wi-Fi le permite conectarse a Internet o con la oficina de una tienda del aeropuerto o el café y le ayuda a mantener la productividad cuando estás fuera de casa. Ahora, imagine que hacer todas estas cosas con facilidad y rapidez - sin preocuparse por la búsqueda de una conexión de red cableada.”<sup>4</sup>

“Aunque se pensaba que el termino viene de **Wireless Fidelity** como equivalente a Hi-Fi, High Fidelity, que se usaba en la grabación de sonido, realmente la WECA contrato a una empresa de publicidad para que le diera un nombre a sus estándar, de tal manera que fuera fácil de identificar y recordar. Phil Belanger, miembro fundador de Wi-Fi Alliance que apoyó en nombre Wi-Fi escribió:

Wi-Fi y el "Style logo" del Ying Yang fueron inventados por la agencia Interbrand. Nosotros (WiFi Alliance) contratamos Interbrand para que nos hiciera un logotipo y un nombre que fuera corto, tuviera mercado y fuera fácil de recordar. Necesitábamos algo que fuera algo más llamativo que “IEEE 802.11b de Secuencia Directa”. Interbrand creó nombres como “Prozac”, “Compaq”, “OneWorld”, “Imation”, por mencionar algunas. Incluso inventaron un nombre para la compañía: “VIVATO”.<sup>5</sup>

Phil Belanger.



Logotipo 1. Logotipo de la Wi-Fi Alliance

<sup>4</sup> [21 de septiembre de 2011, [http://www.wi-fi.org/discover\\_and\\_learn.php](http://www.wi-fi.org/discover_and_learn.php)]

<sup>5</sup>[21 de septiembre de 2011, <http://es.wikipedia.org/wiki/Wi-Fi>]

El termino y el logo Wi-Fi hacen referencia a la Wi-Fi Alliance, la organización que se encarga de certificar los dispositivos inalámbricos para que cumplan con los estándares 802.11 y de esta forma asegurar la interoperabilidad entre dispositivos inalámbricos, mas adelante hablaremos acerca del estándar y la familia 802.11.

### **Bandas de frecuencia.**

Los puntos de acceso que forman parte de la RIU operan en las frecuencias de los 2.4 GHz y los 5 GHz. Si bien estas bandas de frecuencias no requieren licencia, los equipos que las utilicen deben de cumplir con las normas que establezcan los organismos del país donde se encuentren.

En México el organismo que se encarga de controlar el uso y la asignación de frecuencias es la Comisión Federal de Telecomunicaciones (COFETEL), el cual es un órgano desconcentrado de la Secretaría de Comunicaciones y Transporte (SCT). Para el caso de México la norma es la NOM-121-SCT1-2009<sup>6</sup>.

Las bandas de frecuencia son el resultado de la división del espectro electromagnético, con el objeto de delimitar el acceso de usuarios a determinadas bandas. En el espectro electromagnético sabemos que:

- Se marcan todas las frecuencias a utilizar
- Se define su campo de operación
- Se deben de asignar las frecuencias de acuerdo a la normatividad de cada país.

En la banda de los 2.4 GHz hay más problemas de interferencia (pues es la misma banda usada por los teléfonos inalámbricos y los hornos de microondas, entre otros aparatos). Para el caso de la banda de los 5 GHz se presenta menos interferencia. Sin embargo, la utilización de esta banda también tiene sus desventajas, dado que restringe el uso de los equipos con 802.11a a únicamente puntos en línea de vista, con lo que se hace necesario la instalación de un mayor número de puntos de acceso; Esto significa también que los equipos que trabajan con este estándar no pueden alcanzar lugares más lejanos como los del estándar (802.11b/g) dado que sus ondas son más fácil de absorber.

A continuación se muestra una tabla comparativa que nos ayudara a comprender mejor como están asignadas las frecuencias para cada estándar. Además de los canales de operación, el método de transmisión o modulación y la velocidad de acuerdo a cada estándar.

---

<sup>6</sup>[21 de septiembre de 2011, [http://www.cft.gob.mx/work/models/Cofetel\\_2008/Resource/11366/1/images/NOM-121-SCT1-2009.pdf](http://www.cft.gob.mx/work/models/Cofetel_2008/Resource/11366/1/images/NOM-121-SCT1-2009.pdf)]

Estándar 802.11			
Estándar	802.11b	802.11a	802.11g
Frecuencia	2.4 GHz	5 GHz	2.4 GHz
Número de canales	3	Arriba de 23	3
Transmisión	DSS.	OFDM.	OFDM.
Velocidad de transmisión	1, 2, 5.5 y <b>11.</b>	6, 9, 12, 18, 24, 36, 48 y <b>54.</b>	6, 9, 12, 18, 24, 36, 48 y <b>54.</b>

**Tabla 5. Tabla de frecuencias asignadas para los estándares 802.11a/b/g**

Más adelante se describe más a detalle cada uno de los estándares 802.11. En especial los estándares 802.11a, 802.11b, 802.11g y 802.11n. Los cuales estableces las velocidades y la frecuencia de operación para cada estándar.

## **2.4.- Elementos de una red inalámbrica.**

Los elementos que integra una red inalámbrica, está compuesta básicamente de un punto de acceso o AP (por sus siglas en ingles, Access Pint), una antena, la interfaz y el nombre de la red o SSID (por sus siglas en ingles, Service SetIdentifier) a la cual se estable la conexión. En este punto, se describirá la función que juega cada elemento en una red inalámbrica.

### **2.4.1.- Punto de Acceso o Access Point (AP).**

Un elemento fundamental en las redes inalámbricas es el Access Point (AP) o punto de acceso, el cual tiene la función de conectar vario equipos inalámbricos (también denominado “clientes”) entre si y de gestionar al tráfico. El punto de acceso, hace la función de transmisor central y receptor de las señales de radio.

Los puntos de acceso poseen un radio de alcance y una velocidad según la norma que sean definidos, pero existe la posibilidad de instalar una antena externa con el fin de ampliar el área de cobertura.

Los puntos de acceso los podemos clasificar en:

- **AP gordo o inteligente:** son los dispositivos más usados en pequeñas empresas y hogares. Estos equipos realizan todas las tareas de administración.
- **AP delgado o tonto:** normalmente esta clase de equipos son usados para soluciones empresariales. Estos equipos actúan como antenas, llevan una configuración mínima, ya que, la administración la realiza un equipo central, el cual gestiona toda la configuración de la red inalámbrica. Esta solución es perfecta para grandes redes, ya que se pueden ir agregar antenas tantas como consideremos.

### 2.4.2.- Antenas.

Las antenas son dispositivos diseñados con el objetivo de radiar y/o recibir ondas electromagnéticas hacia el espacio libre. Una antena transmisora transforma voltajes en ondas electromagnéticas, y una receptora realiza la función inversa. El tipo de antenas que usamos en los puntos de acceso de la RIU son del tipo omnidireccional y direccional.

- **Antenas Omnidireccionales:** emiten en todas las direcciones, además lo hacen de una forma muy homogénea, es decir, con prácticamente a la misma potencia en todas direcciones. La mayoría de los puntos de acceso vienen con este tipo de antena.
- **Antena Direccional:** como su nombre lo indica, radian la mayor parte de sus energía en una dirección específica, de este modo el patrón de radiación de una antena direccional es muy parecido a un lóbulo.

### 2.4.3.- Tarjeta de Interfaz de Red (NIC).

La tarjeta de red o NIC (Tarjeta de interfaz de red), es la interfaz que permite convertir las ondas electromagnéticas (para el caso de una tarjeta inalámbrica) en datos, los cuales pueden ser procesados por dispositivos tales como laptop, celulares o PDA. De esta forma la tarjeta permite la comunicación con otros dispositivos e intercambiar información.

Cada tarjeta de red tiene un número de identificación único de 48 bits en hexadecimal llamado dirección MAC. Estas direcciones únicas son administradas por el Institute of Electronics and Electric Engineers (por sus siglas en inglés, IEEE). Los tres primeros octetos del número MAC son conocidos como OUI e identifica a los proveedores y son designados por la IEEE. También se denomina NIC al circuito integrado de la tarjeta de red que se encarga de servir como interfaz entre el medio físico (por ejemplo un cable coaxial, cable Ethernet o una antena) y el equipo a través de una antena.

Las tarjetas inalámbricas o wireless, vienen en diferentes variedades dependiendo de la norma a la cual se ajusten, usualmente son 802.11a, 802.11b, 802.11g y 802.11n. La velocidad real de transferencia que llega a alcanzar una tarjeta WiFi con protocolo 802.11b es de unos 11 Mbps y las de protocolo 802.11g llegan como máximo a unos 54Mbps. Actualmente el protocolo que se viene utilizando es 802.11n que es capaz de transmitir a 600 Mbps.



#### 2.4.4.- SSID (Service Set Identifier).

Es el código que llevan los paquetes de una WLAN para identificarlos como parte de la red. Todos los dispositivos de la misma red tendrán que compartir el mismo SSID para poder comunicarse entre sí. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos.

- **ESSID** (Extended Service Set Identifier): es el nombre que se le otorga a la red inalámbrica para diferenciarla de las demás redes de su tipo.
- **BSSID** (Basic Service Set Identifier): se trata de la dirección física (MAC) del Access Point al que se conectan los clientes.

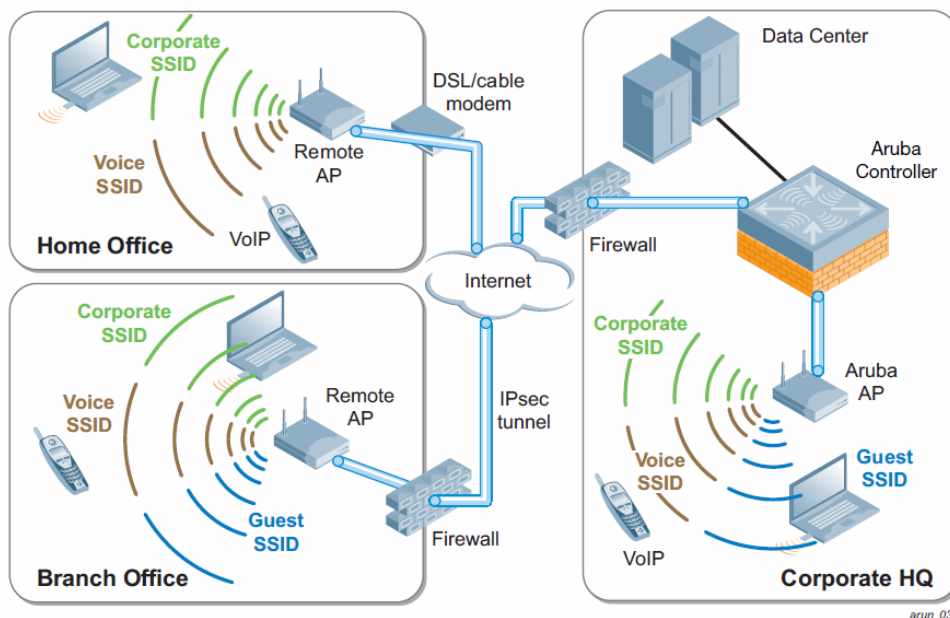


Diagrama 6. Elementos de una red inalámbrica.

#### 2.5.- Estándar IEEE 802.11a/b/g/n

El estándar 802.11 está conformado por varios estándares, de los cuales, nos enfocaremos en los estándares 802.11 /a, /b, g y /n, ya que, estos son los estándares con los que operan los puntos de acceso en la RIU. Como se había explicado al inicio del presente capítulo, la Wi-Fi es la organización que certifica que los equipos cumplan con los requerimientos del estándar 802.11.

Este estándar fue realizado por el Instituto de Ingenieros Eléctricos y Electrónicos o IEEE, y define el uso de los dos niveles más bajo de la arquitectura OSI, especifica sus normas de funcionamiento en una red inalámbrica. Este estándar no es más que la parte

de la norma 802.x encargada de definir la capa de acceso físico (MAC) y de enlace, para entornos que usan ondas radioeléctricas como medio de comunicación. Por esto mismo, los restantes estándares de la familia son complementarios para redes inalámbricas (802.11). Para simplificar esta explicación, podemos decir que una red inalámbrica utiliza el estándar 802.11.

El IEEE ha hecho varias revisiones del estándar 802.11 para mejorar la velocidad de transmisión. Las más utilizadas hasta ahora son /a, /b, /g y /n. IEEE 802.11 es el estándar original sin revisión, que alcanza velocidades máximas teóricas de 2 Mbps. Con el correr del tiempo se fue perfeccionando, lo que implicó que los usuarios debieran cambiar de hardware para poder aprovechar las nuevas características que la norma ofrecía. Actualmente no se encuentra en operación debido a su baja velocidad de transmisión.

### **802.11a.**

IEEE 802.11a: aprobada en 1999, opera en la banda de 5 GHz y utiliza 52 subportadoras operando con Multiplexación División de frecuencia Ortogonal (OFDM) con una velocidad máxima de 54 Mbps. 802.11a tiene 12 canales sin solaparse, 8 para red inalámbrica y 4 para conexiones punto a punto. No puede inter operar con equipos del estándar 802.11b, excepto si se dispone de equipos que implementen ambos estándares.

### **802.11b**

IEEE 802.11b: aprobado en 1999 y, actualmente, el más extendido, opera en la banda de 2.4 GHz y alcanza una velocidad máxima de 11 Mbps. Tiene un radio máximo de 100 metros de cobertura.

### **802.11g.**

IEEE 802.11g: Fue aprobado en el año 2003, posee una velocidad de hasta 54 Mbps y opera en la banda de 2.4 GHz. Es compatible con el estándar /b; de hecho, los equipos con el estándar /b son compatibles, ya que es la evolución del estándar 802.11b. Sin embargo, en redes con el estándar /g la presencia de dispositivos con el estándar /b reduce significativamente la velocidad de transmisión. Suponiendo que se tiene un punto de acceso que trabaja con 802.11g, y actualmente se encuentran conectados un cliente con 802.11b y otro 802.11g, como el cliente 802.11b no comprende los mecanismos de envío de OFDM, el cual es utilizado por 802.11g, se presentarán colisiones, lo cual hará que la información sea reenviada, degradando aún más nuestro ancho de banda

## **802.11n.**

Es el estándar más reciente desarrollado por la IEEE 802.11n, dicho estándar es la actualización del protocolo 802.11. El proyecto es el resultado de años de esfuerzo de estandarizar y actualizar el estándar 802.11g. El estándar 802.11n entrega un nuevo conjunto de características que dramáticamente mejora la fiabilidad de las comunicaciones, la cobertura y el desempeño de los dispositivos.

## **2.6.- Topología de redes inalámbricas.**

Al igual que en las redes cableadas, las redes inalámbricas cuentan con su propia topología; la cual, hace referencia a la disposición física o lógica de una red. En las redes inalámbricas contamos con dos modos de operación.

- Topología Ad-hoc
- Topología Infraestructura

### **2.6.1.- Topología Ad-hoc.**

También conocidas como punto a punto, en la cual, no se requiere de un nodo central o punto de acceso para gestionar el acceso a la red, sino que todos los dispositivos están en igualdad de condiciones. El modo Ad-hoc es el modo más sencillo para el armado de una red. Solo es necesario contar con 2 placas o tarjetas inalámbricas de la misma tecnología. Una vez instaladas en las PC se utiliza un software de configuración del fabricante de la tarjeta inalámbrica para configurarlas en modo ad-hoc.

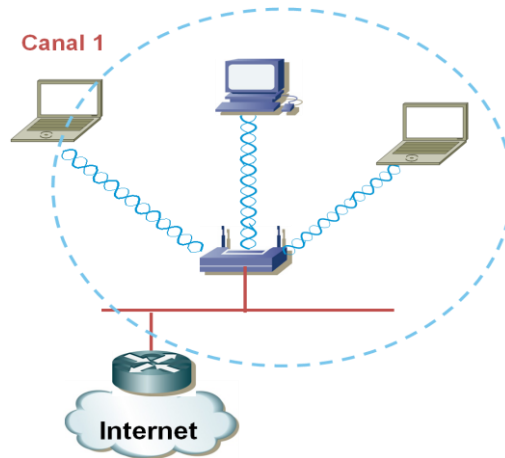
En el siguiente diagrama se muestra una conexión del tipo Ad-hoc, cuya característica principal es que no se necesita un Access Point, ya que esta función está integrada en la tarjeta de red inalámbrica.



**Diagrama 7. Topología en modo Ad-hoc.**

### **2.6.2.- Topología infraestructura.**

En el modo de infraestructura, los dispositivos o “clientes” inalámbricos se conectan a un punto de acceso a través de un enlace inalámbrico. La configuración conformada por el punto de acceso y las estaciones ubicadas dentro del área de cobertura se llama conjunto de servicio básico o BSS, conformando una célula. Cada BSS se identifica a través de un BSSID (identificador de BSS).



**Diagrama 8. Topología en modo Infraestructura.**

### **2.7.- Acceso Múltiple por Detección de Portadora con detección con detección de colisión (CSMA/CD).**

En las redes cableadas existe la técnica llamada CSMA/CD - Acceso Múltiple con Detección de Portadora y Detección de Colisión, la cual permite que múltiples dispositivos utilicen el medio (el cable) para transmitir su información, sin que sucedan colisiones, lo cual causaría la pérdida de datos.

Una colisión ocurre cuando más de un dispositivo intenta enviar información por el medio (el cable) al mismo tiempo. Para evitar esto, CSMA/CD censa el medio para detectar si hay información, de no haber tráfico en el medio se procederá a enviar la información. En caso de que otra máquina no detecte tráfico y esta envíe información, se producirá una colisión y, CSMA/CD establecerá un tiempo aleatorio de espera para cada dispositivo para que vuelvan a tratar de enviar su respectiva información al destinatario.

Un punto de acceso funciona como un Hub, donde todos los dispositivos conectados a este compiten por acceder al medio, y como comparten el mismo medio habrá colisiones. Para solucionar este problema se diseño CSMA/CA.

### **2.8.- Acceso Múltiple por Detección de Portadora con evasión de colisión (CSMA/CA).**

Acceso Múltiple con Detección de Portadora y Prevención de Colisión o CSMA/CA, (por sus siglas en inglés, Carrier Sense Multiple Access Collision Avoidance), es un protocolo de control de redes que permite que múltiples estaciones utilicen un mismo medio de transmisión.

La detección de colisiones no es posible en las redes wireless, porque una estación no puede recibir al mismo tiempo en que transmite, tampoco puede detectar una colisión. En cambio, las redes inalámbricas usan Ready to Send (RTS, Listo para Enviar) y Clear to Send (CTS, Limpio para Enviar) para evitar colisiones.

## **2.9.- Mecanismos de seguridad en las redes inalámbricas.**

La seguridad en cualquier red debe considerarse como parte fundamental del diseño y de la operación. Para el caso de las redes inalámbricas, la seguridad toma un papel fundamental, ya que si confiamos en los métodos de seguridad que viene configurado en los equipos de forma predeterminada, se estaría comprometiendo la integridad de toda la red de una empresa, universidad y/o nuestro hogar.

Las redes inalámbricas hacen uso de las ondas de radiofrecuencia para operar, por lo que es muy complicado delimitar su campo de operación, ya que las ondas de radio se propagan más allá de nuestras instalaciones y cualquier persona ajena a nuestra organización pueden detectar e intentar acceder a ella.

Para prevenir el acceso a personas ajenas de nuestra red, existen métodos de seguridad diseñados especialmente para redes inalámbricas. Estos métodos han ido evolucionando con el tiempo logrando una seguridad más eficiente.

El diseño de una red inalámbrica es fundamental la implementación de seguridad. Antes de implementar una solución para proteger nuestra red primero debemos identificar las amenazas más comunes que podrían afectarnos.

### **2.9.1.- Amenazas de seguridad en redes inalámbricas.**

- **War Driving:** se llama war driving a la búsqueda de redes inalámbricas desde vehículos en movimiento, lo cual implica usar un coche y una laptop para detectar redes sin contraseñas (redes abiertas). El war driving recibe su nombre de war dialing, porque también implica buscar sistemas informáticos y explotar sus debilidades.
- **Hackers:** explotan las debilidades de las redes inalámbricas para introducirse dentro del sistema para demostrar sus habilidades, buscar información o destruirla.
- **Empleados:** la mayor amenaza en una red, ya sea inalámbrica o cableada es llevada por el propio personal que labora en la empresa. Ya que la mayoría de las herramientas de intrusión cada vez son más fáciles de operar y no se requiere gran conocimiento de programación. También dentro de esta categoría tenemos a empleados enojados con la empresa o institución.

Hay varios métodos para mitigar las amenazas de seguridad en las redes inalámbricas.

Control e integridad

- **Autenticación:** asegura que la persona que intenta asociarse a nuestra red es quien dice ser. La cual se realiza por una contraseña. Un método más avanzado es usando un servidor de autenticación, el cual nos pide un nombre de usuario y una contraseña.

Privacidad y Confidencialidad

- **Encriptación:** Protege los datos que son enviados y recibidos durante la sesión establecida con el punto de acceso y el dispositivo.

Protección y disponibilidad:

- **Sistema de Prevención de Intrusos:** son sistemas que mitigan los ataques que intentan acceder al sistema sin autorización.

### 2.9.2.- Mecanismos de seguridad en redes inalámbricas.

A lo largo de los años los métodos de seguridad se han ido perfeccionando. El primer mecanismo de seguridad que se implemento fue Privacidad Equivalente a Cableado o WEP (por sus siglas en inglés, Wired Equivalent Privacy). Este protocolo cuenta con una seguridad básica, ya que sus claves de cifrado tienen una longitud de 64 o 128 bits. El problema del protocolo WEP radica en su cifrado, el cual ha sido descubierto y en internet se puede encontrar gran cantidad de información y programas para vulnerar la seguridad.

El siguiente paso fue Acceso Protegido Wi-Fi o WPA (por sus siglas en inglés, Wi-Fi Protected Access), el cual, se basa en el protocolo de la IEEE 802.11i. Este fue pensado en superar las debilidades de WEP. Este nuevo sistema de seguridad fue creado para ocupar el lugar de WEP mientras se preparaba el estándar 802.11i

Una vez que se ratifico en junio de 2004 el estándar 802.11i, se libero el estándar WPA2 (Wi-Fi Protected Access 2) como un sistema para proteger redes inalámbricas, el cual corrige las vulnerabilidades en WPA. WPA2 no comparte las características con el estándar WPA.

- **WEP:** siglas que hace referencia a un método de encriptación (Wired Equivalent Privacy) creado con el objetivo de generar un estado de seguridad en las conexiones inalámbricas, aunque su cifrado se descubrió muy pronto. Es uno de los tipos de encriptación soportados por la tecnología Wi-Fi. Su codificación puede ir de 64 a 254 bits y esta deshabilitado por defecto. Por la debilidad que implica poseer sólo 24 bits de vector de inicialización, actualmente se le está

reemplazando por WPA. La mayoría de las redes inalámbricas en México hacen uso del estándar WEP.

- **WPA:** es el sucesor de WEP. Este nuevo sistema de seguridad fue creado para ocupar el lugar de WEP mientras se preparaba el estándar 802.11i. Su funcionamiento se basa en utilizar un servidor de autenticación que distribuye claves diferentes a cada usuario, aunque también puede utilizarse como PSK (Pre Shared Key). Usa algoritmo RC4 con una clave de 128 bits (48 bits IV) para cifrar la información.
- **WPA2** (Wi-Fi Protected Access 2): es un sistema para proteger redes inalámbricas, el cual corrige las vulnerabilidades en WPA. WPA2 se basa en el estándar 802.11i y WPA2 no comparte las características con el estándar WPA.
- **802.1x:** Es una norma de IEEE para el control de acceso a una red basada en puertos. Es parte del grupo de protocolos IEEE 802 (IEEE 802.1). Permite la autenticación de dispositivos conectados a un puerto LAN, estableciendo una conexión punto a punto y previniendo el acceso al puerto si la autenticación falla.

## **Capítulo 3. Red Inalámbrica Universitaria (RIU).**

La red inalámbrica fue concebida como una herramienta para la comunidad universitaria (alumnos, académicos y trabajadores), con la cual podrán acceder a internet desde sus dispositivos móviles. El uso de internet como herramienta de trabajo aumenta el desempeño de los usuarios para realizar sus actividades académicas, ya que, nos permite acceder a nuestro correo electrónico, mensajería instantánea, contenido en bibliotecas digitales y diversas herramientas didácticas para cada área de interés.

Actualmente la RIU lleva más de 5 años ofreciendo servicio a la comunidad universitaria. A lo largo de todos estos años la RIU se ha estado renovando para estar al día, en especial en temas referentes a la seguridad y la adaptación de nuevos estándares; por ejemplo, desde el año 2010 la RIU tiene la capacidad de soportar puntos de acceso con el estándar 802.11n.

A finales del año 2010 e inicios del 2011, se han iniciado una serie de pruebas en la RedUNAM con la finalidad de adaptar el protocolo IPv6 a dicha red. En el departamento de la RedUNAM el cual está a cargo del proyecto de la RIU, se han llevado una serie de pruebas para determinar los aspectos necesarios para implementar este nuevo protocolo en la RIU.

### **3.1.- Infraestructura.**

Actualmente, la RIU está presente en la mayoría de las dependencias de la UNAM, la cual tiene presencia en la Ciudad de México y el área metropolitana, así como en diferentes estados de la república mexicana. La siguiente tabla se muestra la cantidad de equipos, así como la distribución de estos.



Switches controladores	Cantidad
Ciudad Universitaria.	5
FES y dependencias externas.	6
Escuelas Nacionales Preparatorias.	9
Colegios de Ciencias y Humanidades.	1
Dependencias Foráneas.	5
<b>Total</b>	<b>26</b>
Puntos de Acceso	Cantidad
Ciudad Universitaria.	545
FES.	102
Dependencias externas.	31
Escuelas Nacionales Preparatorias.	85
Colegios de Ciencias y Humanidades.	34
Dependencias Foráneas.	170
<b>Total</b>	<b>967</b>

**Tabla 6. La tabla muestra los equipos que conforman la RIU.<sup>7</sup>**

Para tener una visión más general de cómo está constituida la RIU, se realizaron los diagramas 9 y 10. Los switches controladores están conectados directamente al “core” o núcleo de la RedUNAM.

<sup>7</sup> [22 de septiembre de 2011. Fuente: <https://www.sbym.riu.unam.mx/riu/inicio.php>]

# RIU

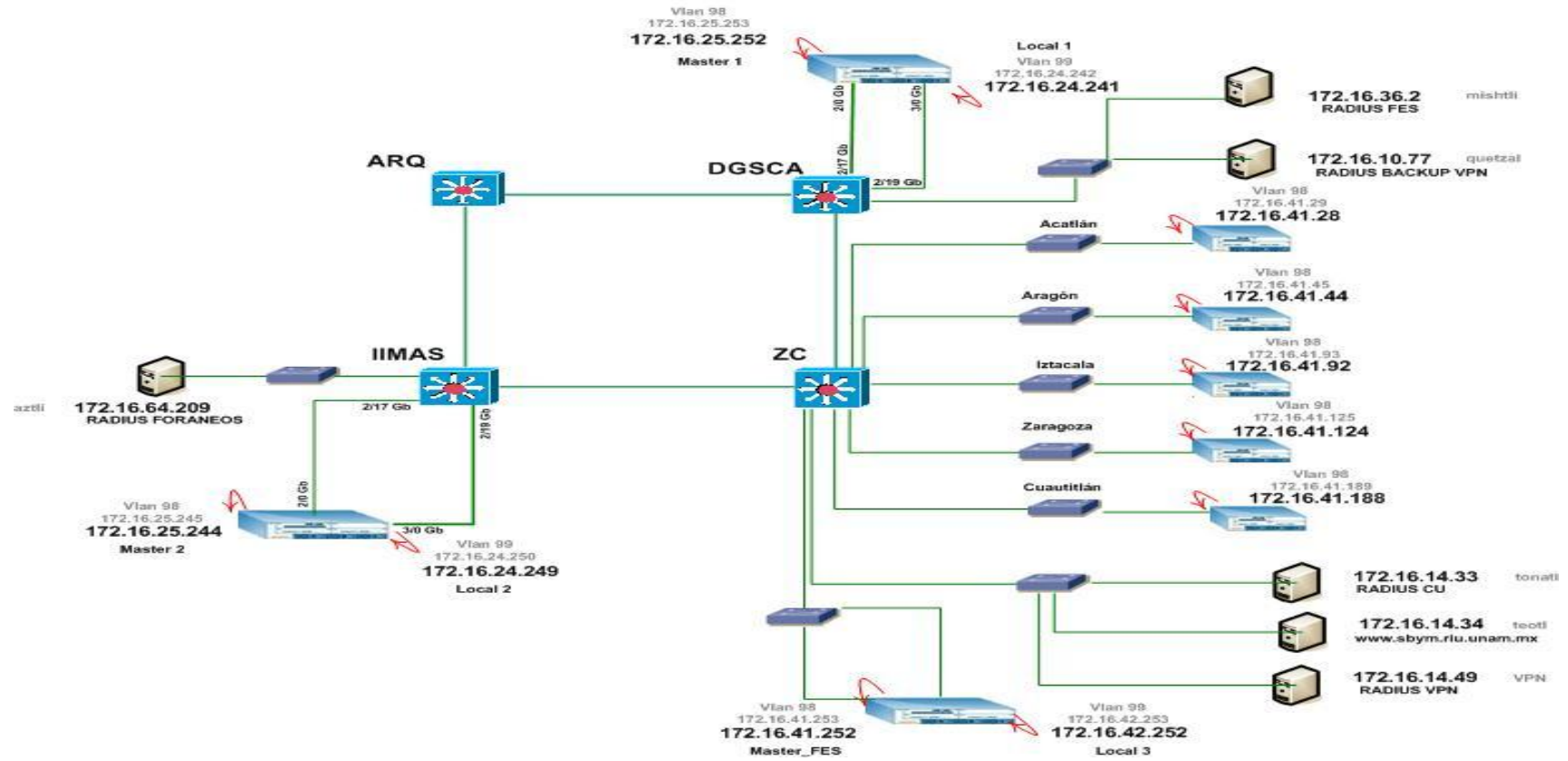


Diagrama 9. Distribución de los switches controladores de la RIU en Ciudad Universitaria.

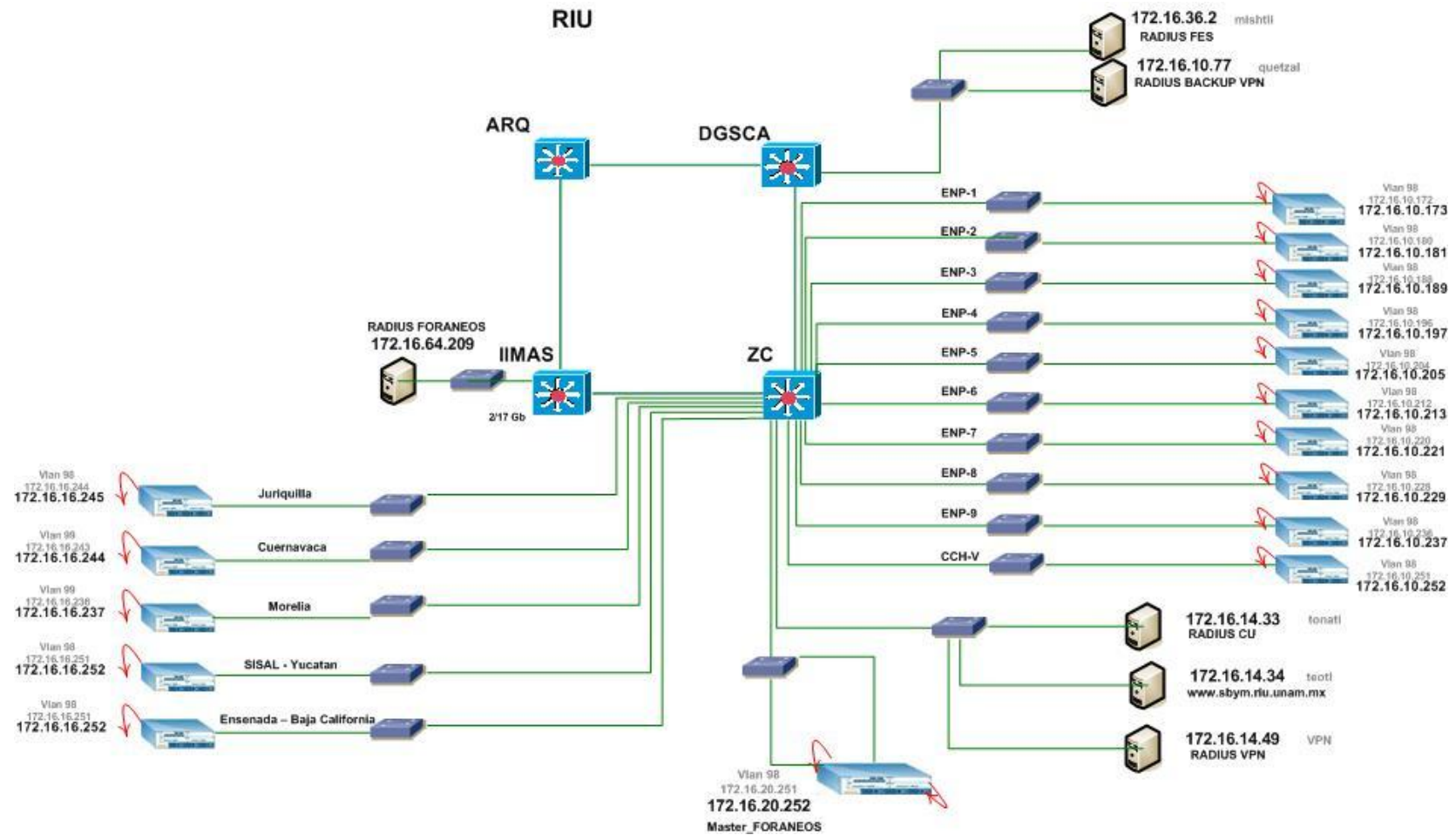


Diagrama 10. Distribución de los switches controladores de la RIU en preparatorias y Campus foráneos.

Además de los switches controladores, también la RIU hace uso de tres servidores de autenticación: mistli, aztli y tonati, los cuales validan las credenciales de los usuarios antes de permitirles el acceso. Se han definido diferentes roles o perfiles, los cuales conllevan ciertos privilegios. Tenemos los roles de: “Staff”, “Académico” y de “Alumno”. El de mayor nivel es para el de “Staff” y con el menor privilegio es para el de “Alumno”.

El crecimiento de la RIU en los últimos años ha crecido de forma considerable, en un principio, era una red inalámbrica de área local dentro de Ciudad Universitaria. Posteriormente paso a ser una red inalámbrica metropolitana, con sus respectivas reservas.

El día de hoy, la RIU se encuentra ofreciendo sus servicios en los campus y centros de investigación fuera del área metropolitana. Las siguientes imágenes ayudan a comprender mejor el crecimiento que ha tenido nuestra Red Inalámbrica Universitaria.

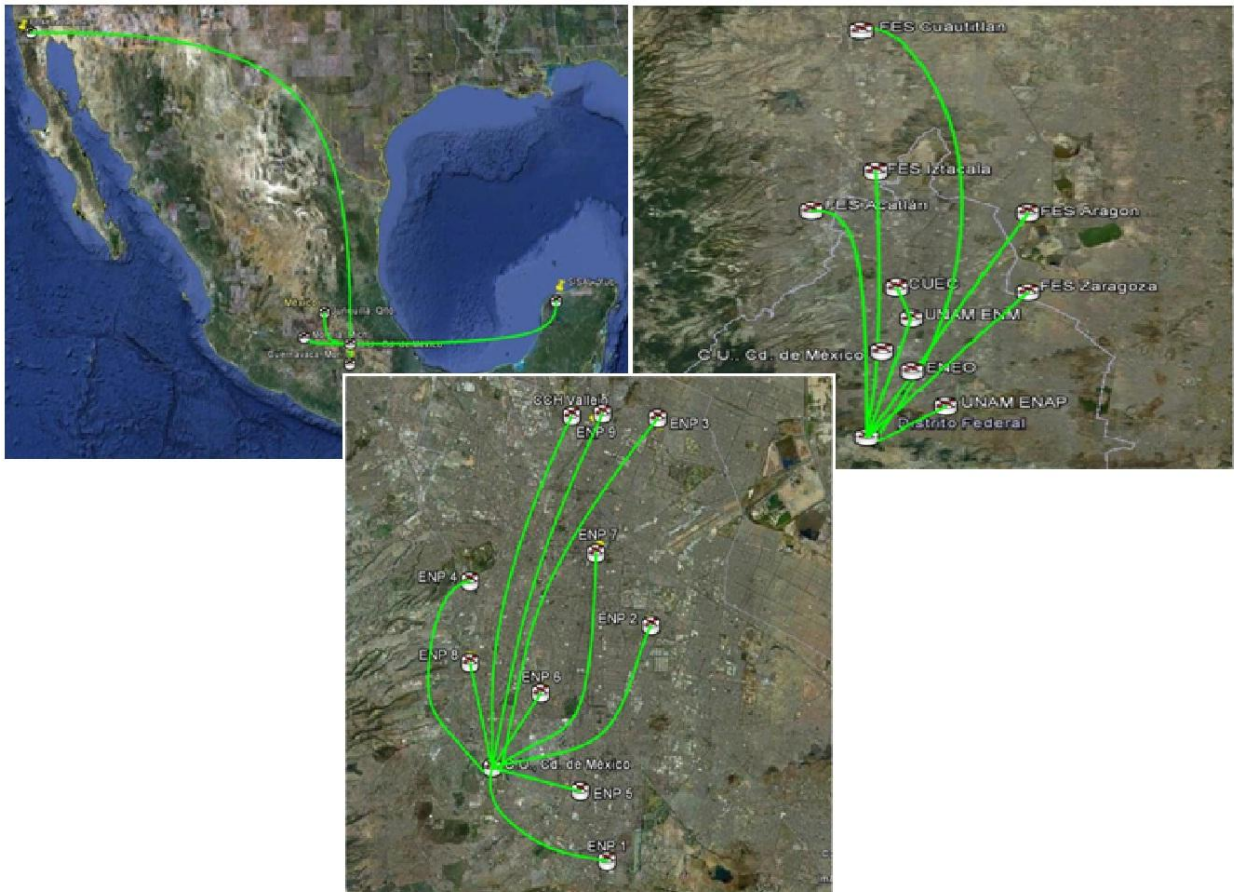


Imagen 1. Presencia de la Red Inalámbrica Universitaria.<sup>8</sup>

<sup>8</sup> Imágenes: Google Earth

### 3.2.- Switch controlador.

El switch controlador es la pieza clave de la RIU, este equipo tiene múltiples funciones, es el encargado de aplicar las políticas del firewall, gestionar el tráfico y administrar cada punto de acceso que este a su cargo.

Este switch controlador tienes tres modos de operar: Standalone, Máster o Local.

En modo Standalone, el propio equipo tiene la función de opera como Máster y Local, lo que también se le conoce como controlador Dual.

En modo Máster, tiene la función de establecer la configuración general, la cual, enviara la configuración a los demás switches que operan en modo “Local”.

En modo Local, tiene la función de administrar el trafico que generan los usuarios, aplicar las políticas del firewall, establecer y gestionar la comunicación con los puntos de acceso por medio del túnel (GRE). Otra función que tiene el local, es servir como equipo de respaldo, el cual aceptara a todos los puntos de acceso y los usuarios cuando el Máster no esté operando.

### 3.3.- Configuración general del switch controlador.

En este apartado se mostrara el archivo de configuración del switch controlador, llamado “Master1”, el cual, está basado en el protocolo IPv4. Debido a que el archivo de configuración es muy extenso, solo se mostrará las partes fundamentales, las cuales, se usarán para realizar las pruebas.

```
(RIU_MASTER1) #show running-config
Building Configuration...
version 3.4
enable secret "*****"
hostname "RIU_MASTER1"
clock timezone PST -8
location "DGSCA"
mms config 0
controller config 1722
ip NAT pool natpool 172.16.250.252 172.16.250.252
ip access-list eth validuserethacl
    permit any
!
```

```

netservice svc-snmp-trap udp 162
netservice svc-sql-udp2 udp 1433
netservice svc-sql-tcp tcp 1434
netservice svc-dhcp udp 67 68
netservice svc-smb-tcp tcp 445
  invert
  network 10.1.0.0 255.255.0.0
  network 10.2.0.0 255.255.0.0
  network 10.3.0.0 255.255.0.0
  network 10.4.0.0 255.255.0.0
  network 10.5.0.0 255.255.0.0
!
netdestination DNS-UNAM
  host 172.16.10.2
  host 172.16.04.1
!
!
netdestination ADMINISTRACION
  network 172.16.120.0 255.255.255.0
  network 172.16.115.0 255.255.255.0
!
netdestination INTERNAL-NETWORK
  network 10.1.0.0 255.255.0.0
  network 10.2.0.0 255.255.0.0
  network 10.3.0.0 255.255.0.0
  network 10.4.0.0 255.255.0.0
  network 10.5.0.0 255.255.0.0
!
ip access-list session SACL-STAFF
  user any udp 68 deny
  any any svc-dhcp permit
  user alias mswitch svc-icmp permit
  user any any src-nat pool natpool
!
!
ip access-list session SACL-ACADEMICO
  user any udp 68 deny
  user any svc-smtp deny
  user any svc-sql-udp2 deny
  user any svc-sql-udp deny
  user any svc-sql-tcp deny
  user any svc-sql-tcp2 deny
  user any udp 161 deny
  user any udp 162 deny
  user any svc-dhcp permit
  user alias mswitch svc-ssh deny
  user alias mswitch svc-http deny

```

```

user  alias mswitch svc-https deny
user  any any src-nat pool natpool
!
!
ip access-list session SACL-OPEN
user  any udp 68 deny
user  any svc-dhcp permit
user  alias mswitch svc-ssh deny
user  alias mswitch svc-http deny
user  alias mswitch svc-https deny
user  any svc-smtp deny
user  any svc-sql-udp2 deny
user  any svc-sql-udp deny
user  any svc-sql-tcp deny
user  any svc-sql-tcp2 deny
user  any udp 161 deny
user  any udp 162 deny
user  any any src-nat pool natpool
!
!
ip access-list session SACL-ESTUDIANTE
user  any udp 68 deny
user  any svc-smtp deny
user  any udp 161 deny
user  any svc-sql-tcp2 deny
user  any svc-sql-tcp deny
user  any svc-sql-udp deny
user  any svc-sql-udp2 deny
user  any udp 162 deny
user  any svc-dhcp permit
user  alias mswitch svc-ssh deny
user  alias mswitch svc-http deny
user  alias mswitch svc-https deny
user  any any src-nat pool natpool
user  any any tcp 9100 deny
!
!
user-role ap-role
!
!
user-role STAFF
session-acl SACL-STAFF
!
user-role ESTUDIANTE
session-acl BLOCK-INTER-USER
session-acl SACL-ESTUDIANTE
!

```

```

user-role logon
!
user-role ACADEMICO
  session-acl BLOCK-INTER-USER
  session-acl SACL-ACADEMICO
!
no spanning-tree
interface mgmt
  dhcp
  shutdown
  ip address 172.16.1.6 255.255.255.240
!
interface loopback
  ip address 172.16.250.252
!
!
vlan 98
vlan 100
!
!
interface gigabitethernet 2/0
  description "gig2/0"
  trusted
  trusted vlan 1-4094
  switchport access vlan 98
!
interface gigabitethernet 2/1
  description "gig2/1"
  trusted
  trusted vlan 1-4094
!
interface vlan 1
  ip address 172.16.0.254 255.255.255.0
  shutdown
!
interface vlan 98
  ip address 172.16.0.253 255.255.255.248
!
interface vlan 100
  ip address 10.1.0.254 255.255.255.0
!
!
!ip default-gateway 172.16.250.254

localip0.0.0.0ipsec
bc0e900ba9addee04a2a055ec75dd6547f731f

```



```

vpdn group l2tp
!
ip dhcp pool vlan100
  default-router 10.1.0.254
  dns-server 132.248.10.2 132.248.204.1
  domain-name riu.unam.mx
  lease 0 2 0
  network 10.1.0.0 255.255.255.0
  authoritative
!
!
mux-address 0.0.0.0
ip domain lookup
!
country MX
aaa authentication mac "default"
!
aaa authentication dot1x "1xP-TERMINATION"
  termination enable
  termination eap-type eap-peap
  termination inner-eap-type eap-mschapv2
!
aaa authentication dot1x "default"
  timer wpa-key-period 2000
  no opp-key-caching
!
aaa authentication-server radius "SRV-TONATI"
  host 172.16.214.33
  key 38387e830c4d0ff
!
aaa server-group "default"
  auth-server Internal
!
aaa server-group "SG-RADIUS"
  allow-fail-through
  auth-server SRV-TONATI
  auth-server SRV-MISHTLI
  auth-server SRV-AZTLI
!
  authentication-dot1x "default-psk"
!
aaa profile "AAAP-OPEN"
  initial-role "OPEN"
!
aaa profile "AAAP-RIU"
  initial-role "ESTUDIANTE"
  authentication-dot1x "default"

```

```

dot1x-default-role "ESTUDIANTE"
dot1x-server-group "SG-RADIUS"
radius-accounting "SG-RADIUS"
!
!
ap system-profile "APSP-LOCAL2"
  lms-ip 172.16.249.249
  bkup-lms-ip 172.16.250.252
!
!
ap system-profile "default"
  bootstrap-threshold 7
!
ap regulatory-domain-profile "default"
  country-code MX
  valid-11g-channel 1
  valid-11g-channel 6
  valid-11g-channel 11
!
!
wlan ssid-profile "SSIDP-OPEN-EVENTOS"
  essid "UNIVERFREE"
!
wlan ssid-profile "SSIDP-OPEN-EVENTOS2"
  essid "DIPLOMADO"
!
!
wlan ssid-profile "SSIDP-RIU"
  essid "RIU"
  opmode wpa-tkip wpa-aes wpa2-aes wpa2-tkip
!
wlan ssid-profile "SSIDP-RIU-WPA"
  essid "RIU-WPA"
  opmode wpa-tkip
!
wlan ssid-profile "SSIDP-RIU-WPA2MIX"
  essid "RIU"
  opmode wpa2-aes wpa2-tkip
!
wlan ssid-profile "SSIDP-RIU-WPAMIX"
  essid "RIU"
  opmode wpa-tkip wpa-aes
!
wlan virtual-ap "VAP-BC"
  aaa-profile "AAP-RIU"
  ssid-profile "SSIDP-RIU-WPAMIX"
  vlan 102-104

```

```
no blacklist
auth-failure-blacklist-time 0
!
wlan virtual-ap "VAP-BN"
  aaa-profile "AAAP-RIU"
  ssid-profile "SSIDP-RIU-WPAMIX"
  vlan 202-203
  no blacklist
  auth-failure-blacklist-time 0
!
wlan virtual-ap "VAP-CA"
  aaa-profile "AAAP-RIU"
  ssid-profile "SSIDP-RIU-WPAMIX"
  vlan 120
  no blacklist
  auth-failure-blacklist-time 0
!
!
ap-group "APG-BN"
  virtual-ap "VAP-BN"
  ap-system-profile "APSP-LOCAL2"
!
ap-group "APG-CA"
  virtual-ap "VAP-CA"
  ap-system-profile "APSP-LOCAL2"
!
ap-name "35.1.1"
  virtual-ap "VAP-OPEN-EVENTOS"
!
ap-name "35.1.2"
  virtual-ap "VAP-OPEN-EVENTOS"
!
ap-name "35.1.3"
  virtual-ap "VAP-OPEN-EVENTOS"
!
!
snmp-server trap disable wlsxAPImpersonation
snmp-server trap disable wlsxAPIinterferenceCleared
snmp-server trap disable wlsxAPIinterferenceDetected
snmp-server trap disable wlsxAPRadioAttributesChanged
snmp-server trap disable wlsxAdhocNetwork
!
process monitor log
end
```

Como se puede observar, el archivo de configuración es muy grande y para poder tener un mejor entendimiento del archivo, se dividió en dos secciones. La primera dedicada a la conectividad de red (configuración física) y la configuración propia de los parámetros de la red inalámbrica (configuración lógica).

**Configuración de Conectividad:** En esta parte se configuran las interfaces de red, las cuales sirven para que el equipo se pueda comunicar con los puntos de acceso y enviar el tráfico de los usuarios hacia internet.

- Interface loopback: Es la dirección IP, la cual buscan los puntos de acceso para bajar su imagen por medio del protocolo TFTP.

```
interface loopback
  ip address 172.16.250.252
```

- Vlan 98: Las Vlan permiten crear redes lógicas, las cuales se les asignan a los grupos que nosotros estemos definiendo según nuestras necesidades. Por ejemplo, para el grupo de la Biblioteca Central (APG-BC) se le puede asignar la vlan 100 y, sucesivamente a cada grupo se le deberá asignar una Vlan.

```
vlan 98
vlan 100
vlan 101
```

- Interface de la Vlan 98: Una vez definidas todas las Vlans, ahora se debe de asignarles una dirección IP a cada una de las Vlan. Para la Vlan de administración (Vlan98) se le asigna una IP homologada, en cambio para las demás Vlan se les asigna direcciones privadas del segmento 10.0.0.0. Por propósitos de seguridad, las direcciones IP homologadas fueron cambiadas por direcciones privadas del segmento 176.16.0.0.

```
interface vlan 98
  ip address 172.16.250.253 255.255.255.248
```

- interface gigabitethernet 2/0: Es la interfaz física del equipo, ya sea en Giga-Ethernet o Fast-Ethernet, la cual se le añade la vlan de administración (Vlan 98).

```
interface gigabitethernet 2/0
  description "gig2/0"
```

```
trusted
trusted vlan 1-4094
switchport access vlan 98
```

- ip default-gateway: es la dirección IP de la puerta de salida, generalmente un router, la cual dará la salida a internet.

```
ip default-gateway 172.16.250.254
```

Estos son los elementos básicos que se deben configurar para que nuestro equipo pueda salir a red.

**Configuración lógica de al red inalámbrica:** En esta sección, se definen varios espectros que permiten establecer la operación de la red inalámbrica.

- netdestination INTERNAL-NETWORK: Es el conjunto o pool de direcciones IP, las cuales estarán disponibles para los clientes, una vez que han sido autenticados.

```
!
netdestination INTERNAL-NETWORK
  network 10.1.0.0 255.255.0.0
  network 10.2.0.0 255.255.0.0
  network 10.3.0.0 255.255.0.0
  network 10.4.0.0 255.255.0.0
  network 10.5.0.0 255.255.0.0
!
```

- ip access-list session SACL-STAFF: Determinan los servicios que estarán disponibles (servicio que especificamos como validos), los cuales podemos aplicar a determinados perfiles o “roles”.

```
ip access-list session SACL-STAFF
  user any udp 68 deny
  any any svc-dhcp permit
  user alias mswitch svc-icmp permit
  user any any src-nat pool natpool
```

- user-role STAFF: Identifica el rol que pueden tener los usuarios, los cuales son “Staff”, “Académico” y de “Estudiante”. A los cuales se les aplicara sus respectivas listas de acceso.

```
!  
user-role STAFF  
  session-acl SACL-STAFF  
!
```

- ip dhcp pool vlan99: Esta sección se definen que bloque de direcciones IP se les proporcionará a los clientes, en relación a cada Vlan que se haya agregado. El pool de dhcp está compuesto por el default router, los DNS y el segmento de red que se define de acuerdo con su respectiva interfaz de Vlan.

```
!  
ip dhcp pool vlan99  
  default-router 10.1.0.254  
  dns-server 172.16.10.2 172.16.204.1  
  domain-name riu.unam.mx  
  lease 0 2 0  
  network 10.1.0.0 255.255.255.0  
  authoritative
```

- aaa profile "AAP-RIU": En estos perfiles se introducen los “User-role”. En este perfil se configuran determinados aspectos de seguridad. El cual nos especifica la forma en que accederemos a la RIU, ya sea por un Captive Portal, una clave compartida, por 802.1x o de libre acceso.

```
!  
aaa profile "AAP-RIU"  
  initial-role "ESTUDIANTE"  
  authentication-dot1x "default"  
  dot1x-default-role "ESTUDIANTE"  
  
  dot1x-server-group "SG-RADIUS"  
  radius-accounting "SG-RADIUS"  
!
```

- wlan ssid-profile “SSIDP-RIU”: Se configuran los nombres de red o SSID que anunciarán los puntos de acceso.

```
!  
wlan ssid-profile "SSIDP-RIU"  
    essid "RIU"  
    opmode wpa-tkip wpa-aes wpa2-aes wpa2-tkip  
!
```

- wlan virtual-ap "VAP-BC": Es la virtualización del punto de acceso, dentro de cual se añade el perfil de AAA, el perfil del SSID y la vlan.

```
!  
wlan virtual-ap "VAP-BC"  
    aaa-profile "AAP-RIU"  
    ssid-profile "SSIDP-RIU-WPAMIX"  
    vlan 310  
    no blacklist  
    auth-failure-blacklist-time 0  
!
```

- ap-group "APG-BC": En esta sección se crean los grupos que se consideren necesarios, además en esta sección añadimos los VAP's que previamente se crearon.

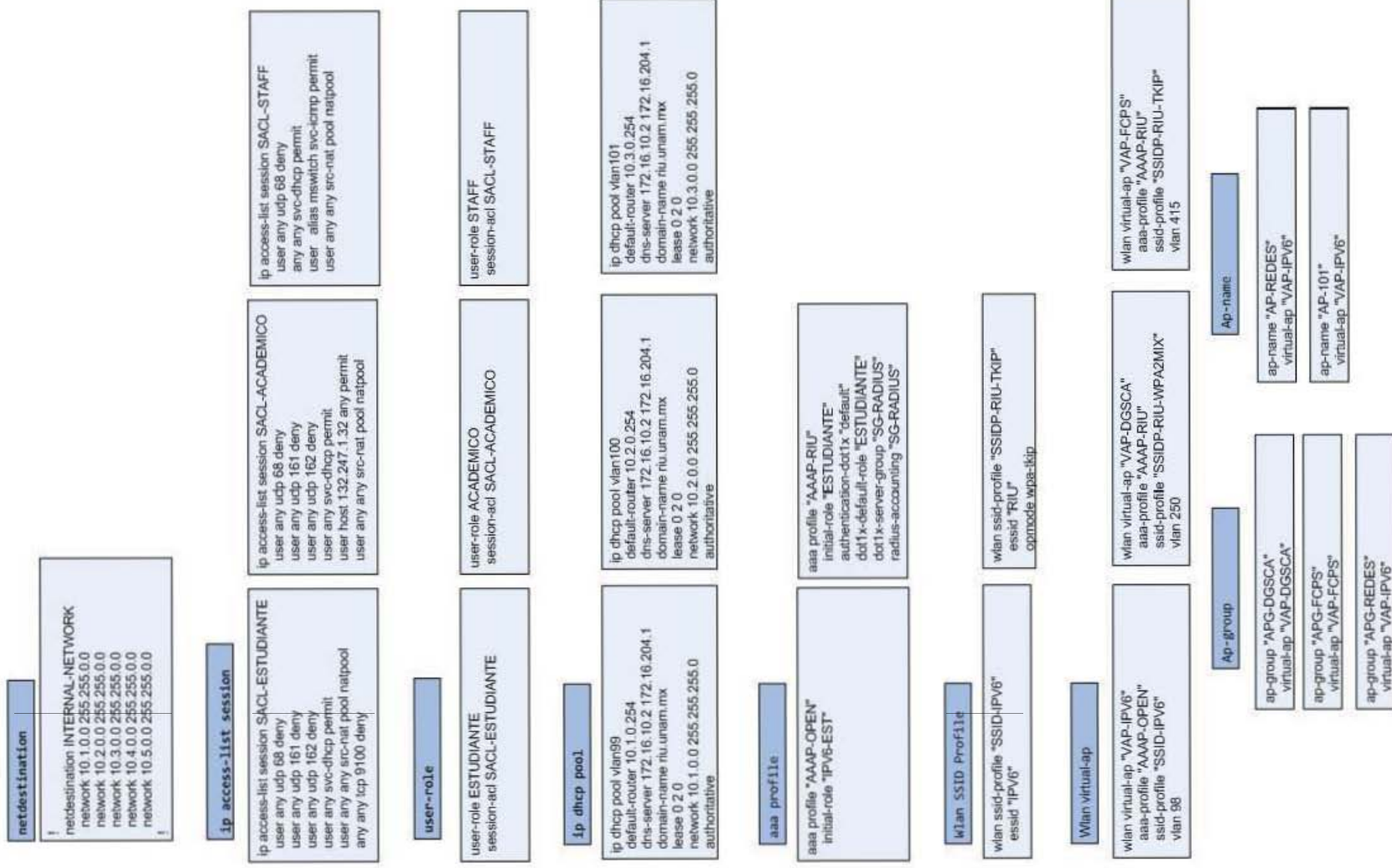
```
!  
ap-group "APG-BC"  
    virtual-ap "VAP-BC"  
    ap-system-profile "APSP-LOCAL2"  
!
```

- ap-name "35.1.3": Es el nombre que identifica a cada punto de acceso, la cual es útil para definir configuraciones individuales o a un grupo de puntos de acceso.

```
!  
ap-name "35.1.3"  
    virtual-ap "VAP-OPEN-EVENTOS"  
!
```

### 3.4.- Esquema de configuración lógica.

El siguiente esquema representa un resumen de la configuración lógica del switch controlador. Este resumen representa la configuración lógica de la RIU.



Esquema 1. Configuración lógica del switch controlador.



## Capítulo 4. Protocolo IPv6.

A finales de los años 80's ya se vislumbraba el problema con el direccionamiento IPv4; el agotamiento de direcciones, debido principalmente al crecimiento de Internet. El desarrollo del protocolo inicio a principios de la década de los 90's y, para el 17 de noviembre de 1994<sup>9</sup> se aprobó el estándar por el Grupo Gestor de Ingeniería de Internet IESG (por sus siglas en inglés, Internet Engineering Steering Group). El cual tiene como objetivo adoptar el protocolo IPv6 en la infraestructura actual y de esta forma, hacer frente al agotamiento de direcciones que se presenta en estos momentos.

En primera instancia, se desarrollaron diferentes técnicas mientras se diseñaba un nuevo protocolo que solucionara estos problemas. Como ejemplo tenemos la técnica de Mascara de Longitud Variable o VLSM (por sus siglas en inglés, Variable Length Subnet Mask), la cual hace mejor uso del direccionamiento. Otra técnica que ha sido de gran ayuda es la Traducción de Direcciones de Red o NAT, la cual permite a varios dispositivos con direccionamiento privado salir a Internet a través de una dirección válida.

En este capítulo se verán las características y ventajas que nos ofrece el protocolo de Internet versión 6.

### 4.1.- Introducción al protocolo IPv6.

Como comentábamos anteriormente, el protocolo IPv6 se desarrollo para sustituir al protocolo IPv4, en primera instancia, habrá una transición paulatina para posteriormente pasar a la sustitución. Más adelante se verán las técnicas de transición.

El protocolo IPv6 nos asegura el crecimiento de Internet para las próximas décadas, ya que, el protocolo IPv4 usa 32 bits para definir las direcciones, con lo cual obtenemos el total de  $2^{32}$  (aproximadamente 4 mil millones de direcciones), las cuales no son suficiente para los requirentes actuales. Para ello, IPv6 usa 128 bits para definir las direccione, de esta manera obtendríamos aproximadamente  $2^{128}$  o 340 trillones de trillones de direcciones.

Por lo tanto, el protocolo IPv6 ofrece una gran cantidad de direcciones, lo suficiente como para otorgarle de tres a diez direcciones IPv6 a cada habitante del planeta, de tal modo se permitirá que millones de dispositivos (laptop, celulares, PDAs y tablets) estén siempre conectados o en "línea".

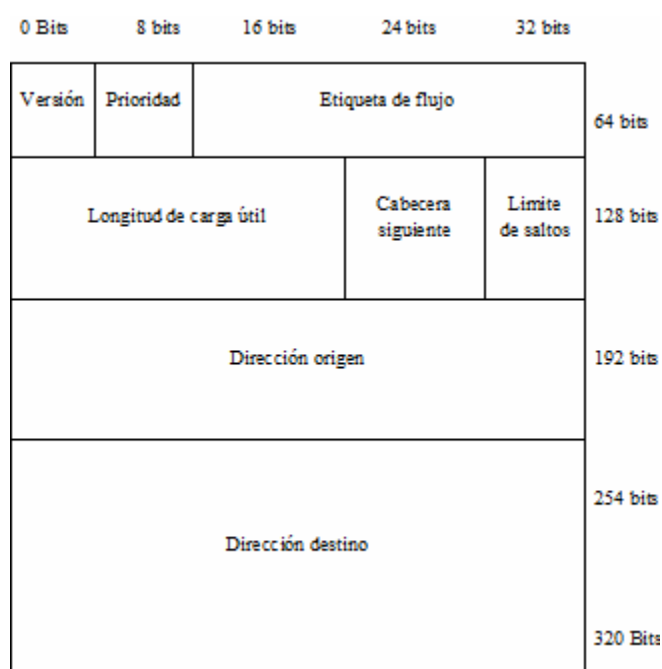
---

<sup>9</sup> <http://www.ipv6.unam.mx/historia.html>

## Características principales.

- Mayor espacio de direcciones. El tamaño de las direcciones IP cambia de 32 bits a 128 bits.
- Simplificación del formato de Header. Algunos campos de header IPv4 se quitan o se hacen opcionales
- Paquetes IP eficientes y extensibles, sin que haya fragmentación en los routers, alineados a 64 bits.

## 4.2.- Cabecera del protocolo IPv6.



Cuadro 16. Cabecera del protocolo IPv6.

- Versión: Identifica la versión del paquete (IPv6)
- Prioridad: Se usa para distinguir entre paquetes a cuyas de orígenes se les puede controlar el flujo y aquellos a los que no.
- Etiqueta de Flujo: Aún es experimental, pero se usará para permitir a un origen y A un destino establecer una pseudo conexión con prioridades y requisitos Particulares.
- Longitud de Carga Útil: Indica cuantos bytes siguen en la cabecera de 40 bytes.
- Campo de Siguiente Cabecera: Indica las cabeceras de extensión, de haberlas, Sigue a ésta. (Cabeceras de extensión: Opciones salto por salto; enrutamiento; Fragmentación; verificación de autenticidad; carga útil cifrada de seguridad; Opciones de destino).

- Límite de Salto: Indica el número máximo de saltos que un paquete puede pasar De un router a otro.
- Campo de Dirección de Origen.
- Campo de Dirección de Destino.

### 4.3.- Formato del direccionamiento IPv6.

Como se comento anteriormente, una de las diferencias entre el protocolo IPv4 y el protocolo IPv6, es la cantidad de bits usado para definir las direcciones. Las direcciones en IPv6 se representan en formato hexadecimal y se usan los dos puntos para separar la dirección en 8 campos de 16 bits cada una.

Cada dígito hexadecimal se asocia con 4 bits, cada campo de 4 dígitos en hexadecimal serán 16 bits por campo. Si multiplicamos los 16 bits por los 8 campos que conforman la dirección, nos da un total de 128 bits.

Un ejemplo de dirección IPv6 es el siguiente:

**2001:0000:0001:0002:0000:0000:0000:ABCD**

Como se puede ver, la dirección en IPv6 es más extensa que una dirección del protocolo IPv4. Para resolver en alguna medida esta situación, contamos con dos condiciones para simplificar la gran cantidad de número y tener una mejor comprensión del direccionamiento.

- Todos los **0** a la izquierda de cada uno de los campos pueden ser omitidos

**2001:0:1:2:0:0:0:ABCD**

- Se pueden omitir los campos consecutivos de 0 con “::” independientemente de la cantidad de campos que se abrevie. Este mecanismo sólo puede hacerse una vez debido a que luego no se podrían reestructurar la cantidad de campos exactamente como eran.

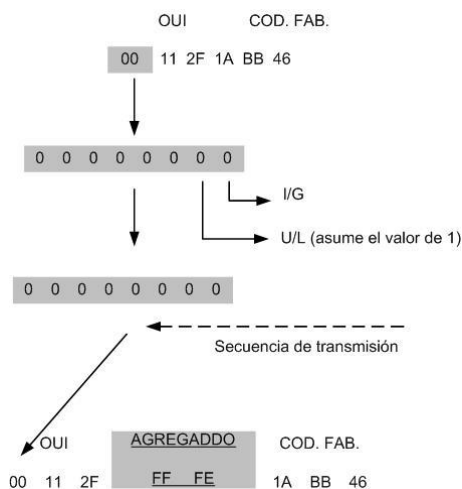
**2001:0:1:2::ABCD**

## Identificadores de las interfaces.

Los ID de una dirección IPv6 son utilizados para identificar de manera única una interfaz, este segmento de la dirección es llamada porción de host. Estos ID deben ser únicos en los enlaces, tienen una longitud de 64 bits y pueden ser creados dinámicamente basándose en las direcciones de la capa de enlace.

El tipo de capa de enlace determinará cómo son dinámicamente creadas las interfaces de IPv6 y cómo funcionará la resolución del direccionamiento, Para Ethernet la interfaz ID está basada en la dirección MAC de la interfaz en un formato llamado EUI-64 (Extended Universal Identifier 54-bits). Este formato deriva de la dirección MAC de 48 bits con el agregado de los números hexadecimales **ffe** entre el OUI y el código de vendedor. El séptimo bit del primer byte del ID de la interfaz resultante corresponde al bit *universal local* (U/L) asume el valor binario 1. Este bit indica si la interfaz ID es localmente única en ese enlace o universalmente única.

El octavo bit en el primer byte de la interfaz ID corresponde al *individual/group* (I/G) que se utiliza para gestionar grupos multicast, en ese caso no varía.



Esquema 2. IPv6 Interfaz ID.

Ethernet transmite los bits de bajo orden de cada byte primero (a la inversa) el bit U/L es el bit séptimo y el I/G es el octavo de la dirección, por lo tanto el primer bit de la dirección MAC transmitida será el bit I/G, usado por direcciones broadcast y multicast y el segundo bit transmitido será el U/L.

#### 4.4.- Direccionamiento en IPv6.

Como se había visto en el primer capítulo, los host en IPv4 usan diferentes modos de comunicación para establecer la comunicación con otros dispositivos y se cuenta con tres tipos de direccionamiento: Unicast, Broadcast y Multicast.

Para el caso del protocolo IPv6 también contamos con tres tipos de direccionamiento:

- **Unicast:** Este tipo de direcciones identifica de forma única a una interfaz. Los datos son enviados únicamente a la interfaz identificada con dicha dirección. En IPv6 contamos con varios tipos como: link local, site local y global.
- **Anycast:** Este tipo de direcciones identifica a un conjunto de dispositivos. Un paquete que es enviado a una dirección identificada como Anycast, es reenviada a una de las interfaces identificadas por esa dirección. A este tipo de direccionamiento también se le conoce como “uno al más cercano”.
- **Multicast:** Una dirección multicast identifica a un conjunto de direcciones en diferentes dispositivos. Un paquete que se envié a una dirección multicast es reenviada a todas las interfaces identificadas por esa dirección. Lo que permite establecer la comunicación de uno a muchos.

##### 4.4.1.- Unicast.

Existen varios tipos de direcciones IPv6 unicast.

- Global: Inician con 2000::/3
- Link-local (Privadas): Inicia con FE80::/10
- Loopback: (::1)
- Reservada: usada por la IETF
- Sin especificar. (::)

##### Dirección IPv6 Global.

La escalabilidad de la red es sumamente importante, es directamente proporcional a la capacidad de sumarización que tiene la red. Tal como ocurre con IPv4 los bits más a la izquierda indican el prefijo de enrutamiento y pueden ser sumarizados. Teóricamente existen  $2^{64}$  prefijos IPv6. Si cada prefijo fuera almacenado en la memoria del router utilizando 256 bits (32 bytes), entonces la tabla de enrutamiento consumiría  $5.9 \times 10^{20}$  bytes,

lo cual es demasiado. Esto se reduce a la importancia que tiene la sumarización al momento de construir la tabla de enrutamiento.

En el siguiente cuadro se muestra un direccionamiento Global IPv6, definido por la RFC 3587.

Global Prefix	Subnet ID	Interface ID
	/ 48	/64

**Cuadro 17. Longitud de una dirección en IPv6.**

Los primero 48 bits de la dirección Global IPv6 son utilizados para enrutamiento en Internet en el ISP, los siguientes 16 bits forman el sub-net ID permitiendo así a una empresa subdividir su red. Los restantes 64 bits son la interfaz ID en formato EUI-64.

La IANA está asignando direcciones que comienzan con el valor binario 001 o 2000::

Por ejemplo un ISP podría disponer a una organización de la siguiente dirección 2001:0:1AB::

### **Dirección IPv6 Link local.**

Las direcciones unicast de IPv6 locales, permiten a dispositivos que estén en la misma red local comunicarse sin necesidad de asignación de un direccionamiento global. Las direcciones locales son utilizadas para el enrutamiento y por los procesos de descubrimiento entre protocolos. Son auto configuradas utilizando el prefijo FE80::

10 bits	54 bits	64 bits
<b>1111 1110 10</b>	<b>0</b>	<b>Interface ID</b>
FE80::/10		

**Cuadro 18. Formato de dirección Link-local.**

Por ejemplo, una MAC 00-0F-66-81-19-A3 tendrá una dirección IPv6 Local FF80:020F:66FF:FE81:19A3.

La RFC 4291 especifica otro tipo de dirección unicast. Las direcciones IPv4 son mapeadas a IPv6 concatenando la dirección 0::FFFF:0:0/96 con una determinada dirección IPv4. Por ejemplo la dirección 10.0.0.1 se convierte en 0::FFFF:A00:1, debido a que 10.0.0.1 es en hexadecimal 0A00:0001. Estas direcciones pueden ser utilizadas por los host dual stack, que son aquellos que utilizan ambos tipos de direccionamiento.

### **Dirección de Loopback.**

Del mismo modo que en el direccionamiento en IPv4, que dispone de una dirección especial. Para el caso de IPv6, también se ha dispuesto de una dirección de loopback para realizar las respectivas pruebas. A diferencia de la dirección o direcciones de loopback de IPv4, en IPv6, solo hay una sola dirección y no un bloque entero. La dirección de loopback es 0:0:0:0:0:0:0:1, también expresada comúnmente como “::1” (usando la compresión de ceros).

### **Dirección si especificar.**

En IPv4, cuando tenemos una dirección en ceros (0.0.0.0) se refiere al host a sí mismo, la cual es una dirección reservada por la IANA. La cual es usada por el propio host cuando no conoce su propia dirección. Para IPv6, también se definió una dirección sin especificar, que se suele usar en el campo de origen de un datagrama que es enviada por el dispositivo que busca obtener su dirección IP configurada. La dirección se define dejando en ceros 0:0:0:0:0:0:0:0, también expresada comúnmente como “::” (usando la compresión de ceros).

#### 4.4.2.- Anycast.

Una dirección de este tipo es una dirección global que se está asignando a dos o más host. Los dispositivos enrutan hacia la dirección más cercana utilizando la métrica proporcionada por el protocolo de enrutamiento.

La siguiente figura muestra dos rutas hacia un ISP, ambos routers llevan configuradas la misma dirección IPv6 anycast. Los routers internos simplemente enrutan al cliente hacia el router más cercano al ISP, en este caso el router **A**. La redundancia hace que el router **B** se active y que los routers internos converjan hacia él en el caso de que el router **A** falle.

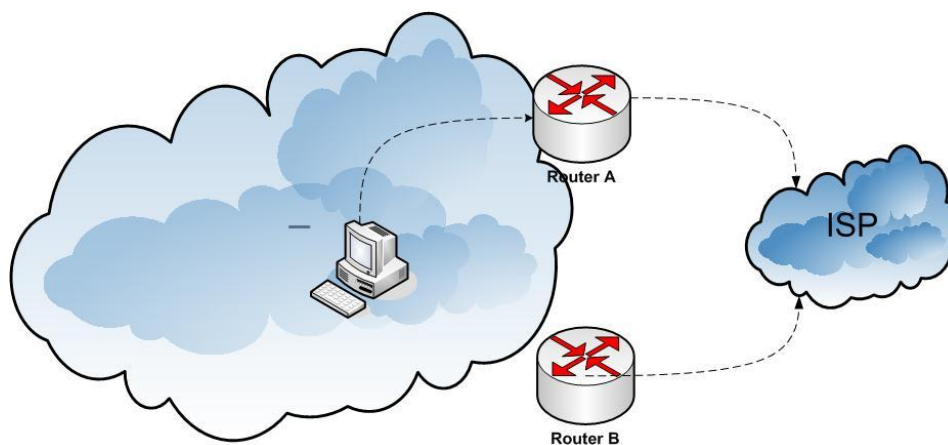


Diagrama 11. Ejemplo del funcionamiento de Anycast.

Una interface puede tener varias direcciones y de diferentes tipos. Los routers tienen que reconocer estas direcciones incluyendo las de anycast y multicast.

Las direcciones anycast son creadas asignando la misma dirección a más de un dispositivo. No existe un espacio de direccionamiento designado para anycast. Los dispositivos que emplearán este tipo de direcciones deben ser explícitamente configurados y tiene que saber que la dirección es de anycast.

Todos los router tienen que soportar la dirección anycast *subnet-router* para las subredes en las cuales tienen interfaces. Estas direcciones son las direcciones de unicast con la porción de la interfaz ID puesta en 0. Los paquetes enviados a la dirección de anycast *subnet-router* serán entregados a un router específico en la subred.



### 4.4.3.- Multicast.

Una dirección de multicast identifica a un grupo de interfaces. El tráfico enviado al grupo llega a todas estas interfaces. Estas pueden a su vez pertenecer a varios grupos multicast simultáneamente. Cada interfaz puede reconocer varias direcciones de multicast incluyendo la dirección *all-nodes*, la dirección *solicited-nodes* o cualquier otra dirección a la que el nodo pertenezca. Los routers deben ser capaces de reconocer la dirección *all-routers*.

El formato de una dirección IPv6 de multicast se ilustra en la siguiente figura:

8 bits	4 bits	4 bits	112 bits
<b>1111 1111</b>	<b>Flag</b>	<b>Scope</b>	<b>Group ID</b>
FF::/8			

Cuadro 19. Formato de dirección multicas para IPv6.

Las direcciones de multicast están en el rango **FF00::/8**, todas las otras direcciones IPv6 están en el espacio de direccionamiento unicast. Las direcciones de broadcast no existen en IPv6. En todo caso un direccionamiento especial de multicast podría ser considerado como broadcast, donde todos los dispositivos están interesados en recibir ese tráfico.

Como se muestra en la figura la dirección IPv6 multicast comienza con el prefijo FF00::/8 los siguientes 4 bits son identificadores que se describen a continuación.

1. El primer identificador o bandera es indefinida y siempre tiene el valor de cero.
2. Conocido como el bit “**R**” tiene el valor en binario de 1, cuando el RP esté contenido en el paquete multicast.
3. Conocido como el bit “**P**” lleva el valor binario 1 en el caso de que la dirección multicast esté basado en un prefijo unicast.
4. Es el llamado bit “**T**”, si la dirección esta asignada permanentemente lleva el valor 0, si por el contrario el valor es 1 la dirección es temporal.

Los 4 bits después de las banderas indican el ámbito de la dirección limitando cuán lejos esta dirección multicast es capaz de llegar. En IPv4 se utiliza el TTL para poder efectuar esta tarea pero no es un mecanismo exacto debido a que la distancia permitida por el TTL puede ser demasiado larga en una dirección y demasiado corta en otra. El ámbito en IPv6 es lo suficientemente flexible como para limitar multicast en un sitio o una empresa determinada.

Los ámbitos están definidos en hexadecimal y son los siguientes:

- Valor 1: ámbito interfaz-local, usado para las interfaces loopback.
- Valor 2: ámbito link-local, similar al ámbito unicast link-local.
- Valor 4: ámbito admin-local; debe ser administrativamente configurado.
- Valor 5: ámbito site-local; sólo abarca un sitio.
  
- Valor 8: ámbito organization-local; abarca varios sitios pertenecientes a múltiples sitios u organizaciones.
- Valor E: es de ámbito global.

El ID del grupo multicast son los 112 bits de menor ámbito de la dirección.

Todos los dispositivos deberían reconocer y responder a estas direcciones multicast de todos los nodos:

- **FF01::1** correspondiente a la interfaz local.
- **FF02::1** correspondiente al enlace local.

Las direcciones de multicast *solicited-nodes* son utilizadas en los mensajes de solicitud de vecinos y son enviados en un enlace local por un dispositivo que quiere determinar la dirección de la capa de enlace de otro dispositivo en el mismo enlace local. Estos mecanismos se asemejan a ARP en IPv4. Una dirección de multicast *solicitud-nodes* comienza con el prefijo **FF02::1:FF00:/104** y en los últimos 24 bits insertando las direcciones unicast o anycast del dispositivo.

Los router deben poder responder a las direcciones multicast *all-router*:

- **FF01::2** es la dirección de la interfaz local.
- **FF02::2** es la dirección de enlace local.
- **FF05::2** es la dirección del sitio local.

Los router también se unen a otros grupos para soportar protocolos de enrutamiento como por ejemplo, OSPF versión 3 (OSPFv3) utiliza **FF02::5** y **FF02::6**, y RIPng (Routing Information Protocol new generation) utiliza **FF02::9**.

#### 4.5.- Asignación de direcciones IPv6.

Las direcciones IPv6 pueden ser asignadas de manera manual, de forma dinámica usando DHCPv6 o autoconfiguración por stateless.

##### 4.5.1.- Manual.

El administrador es el encargado de asignarlas y configurarlas manualmente, supone más trabajo y demanda llevar un registro de las direcciones que han sido asignadas y a que host.

##### 4.5.2.- Autoconfiguración Stateless.

Cada router anuncia información de red incluyendo el prefijo asignado a cada una de sus interfaces. Con la información contenida en este anuncio los sistemas finales crean una dirección única al concatenar el prefijo con el ID en formato EUI-64 de la interfaz. El nombre stateless viene de que ningún dispositivo lleva un registro de las IP que se van asignando. Los sistemas finales piden información de red al router usando un mensaje específico denominado **Router Solicitation** y los routers responden con un mensaje **Router Advertisement**. Existe un proceso denominado **DAD** (Duplicate Address Detection), que se encarga de verificar que las IPs no estén en uso y que no sean duplicadas.

#### 4.6.- Direcciones IPv6 reservadas.

Existen direcciones IPv6 reservadas que no pueden utilizarse para direcciones unicast convencionales, las más importantes son:

::/128	Dirección no especificada, equivalente a 0.0.0.0 de IPv4
::1/128	Dirección de loopback, equivalente a 127.0.0.1 de IPv4
fc00::/7	Equivalente a las direcciones especificadas en RFC1918 de IPv4.

Se dividen en dos grupos:

fc00::/8	Se asignar de forma centralizada a través del denominado “ULA-Central”
fd00::/8	Se construye generando una cadena de 40 bits aleatoria, tal como se define en el RFC4193

ff00::/8	Direcciones multicast, equivalente al rango 224.0.0.0/4 de IPv4
fe80::/10	Direcciones link-local, equivalente al rango 169.254.0.0/16 de IP IPv4

Tabla 7. Direccionamiento reservado.

#### **4.7.- Técnicas de transición.**

Para llevar a cabo la implementación del protocolo IPv6 en nuestra infraestructura, contamos con un conjunto de mecanismos de transición. Los cuales nos ayudaran en la transición de forma paulatina, ya que, la meta principal es pasar del protocolo IPv4 al protocolo IPv6 de forma nativa con la menor interrupción posible.

Para realizar la transición del IPv4 a IPv6 contamos con dos mecanismos:

**Dual Stack:** La cual provee soporte para IPv4 e IPv6 en los host así como en los routers.

**Tunneling:** Esta técnica se basa en la encapsula los paquetes IPv6 dentro del encabezado del protocolo de IPv4. Los datos viajan a través de una infraestructura de IPv4 (los router y los host no soportan de forma nativa IPv6 en sus interfaces).

##### **4.7.1.- Dual Stack.**

En el mecanismo Dual Stack, las interfaces de los equipos tiene la capacidad de enviar y recibir paquetes IPv4 e IPv6, de esta forma se logra la comunicación con equipos IPv4 usando paquetes IPv4, y de la misma forma comunicarse con equipos en IPv6 usando paquetes IPv6.

Dual Stack nos permite realizar la transición al protocolo IPv6, para ello, los equipos o host deben soportar en sus interfaces ambos protocolos. Actualmente la mayoría de los sistemas operativos en sus últimas versiones (Linux, Windows y MAC) cuentan con soporte para IPv6.

Para el caso de los equipos de telecomunicaciones (router y switches), la transición es más compleja. El principal factor es el costo, ya que, la mayoría de estos equipos que están en operación son muy viejos y no soportarían una actualización.

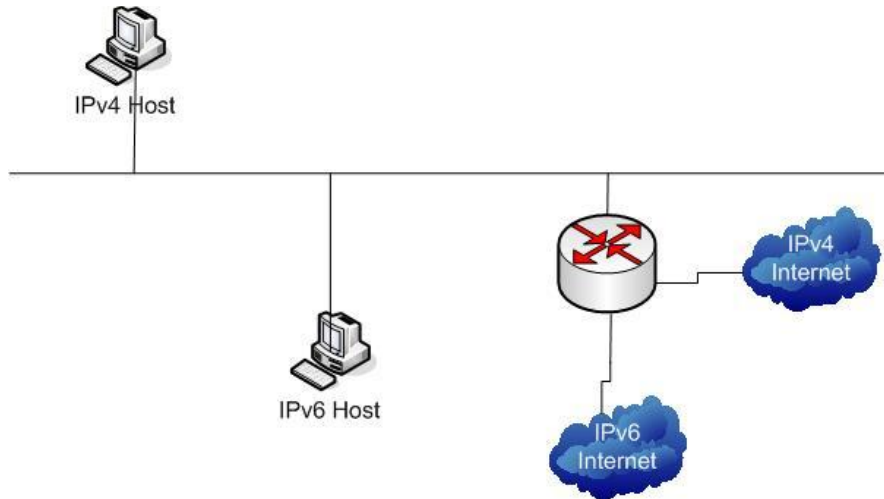
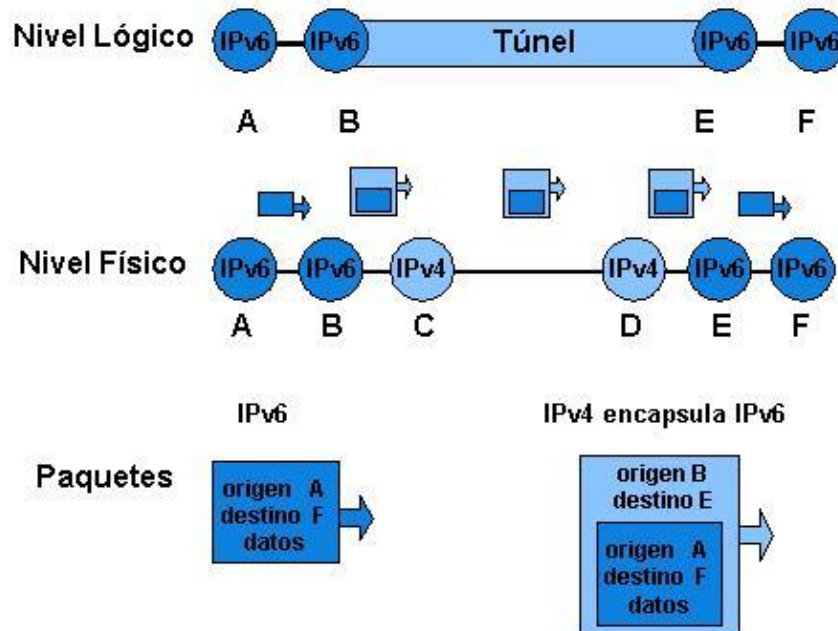


Diagrama 12. Ejemplo del funcionamiento de dual-stack en una red.

#### 4.7.2.- Tunneling.

Como habíamos comentado anteriormente, el mecanismo de Tunneling nos ayuda en la transición, la cual se basa principalmente en establecer un túnel para enviar paquetes de IPv6 sobre una infraestructura en IPv4, el cual crea un enlace virtual o túnel entre ambos equipos. Tanto los host y los routers deben contar con sus respectivas direcciones en IPv4 e IPv6.



Fuente: [ <http://www.rau.edu.uy/ipv6/queesipv6.htm> ]

Esquema 3. Mecanismo Tunneling.

Para establecer la comunicación por medio de túneles contamos con las siguientes técnicas:

- **Tuneling manual IPv6-to-IPv4:** Es un método de integración en el cual, los paquetes de IPv6 son encapsulados dentro del protocolo de IPv4. En este método se requiere que los routers sean dual-stack.
- **Tunneling dinámico 6to4:** Es un método que automáticamente establece la conexión, enviando paquetes en IPv6 a través de una red en IPv4, sin la necesidad de configurar túneles manualmente. La cual permite una rápida implementación de una red IPv6 sin obtener la dirección del ISP
- **Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunneling:** Es un mecanismo automático que cubre un túnel que usa una red IPv4 subyacente como un enlace para IPv6. Los túneles ISATAP permiten a host individuales con IPv4 o IPv6 con dual-stack dentro de un site comunicarse con otros host en un enlace virtual, creando una red IPv6 usando la infraestructura de IPv4.
- **Tunneling Teredo:** Es una tecnología de transición a IPv6 que provee un túnel de forma automática de host-to-host en lugar de usar túnel como puente. Es usado para pasar trafico unicast de IPv6 cuando los host con dual-stack (host que usan tanto el protocolo IPv4 como IPv6) están detrás de uno o más NAT.

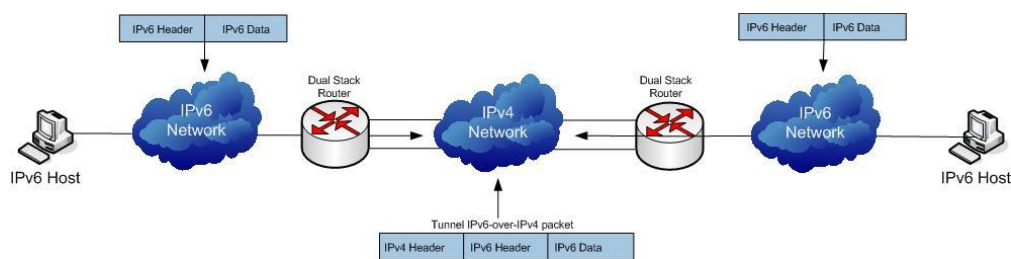


Diagrama 13. Ejemplo del funcionamiento de la técnica del Túnel.

## **Diferencia entre el protocolo IPv4 e IPv6.**

Las diferencias entre ambos protocolos, se pueden observar al comparar los encabezados. El IPv6 es más simple que su contraparte, al tener menor cantidad de campos, el procesamiento es más rápido facilitando el enrutamiento.

En IPv4 es normal asignar una dirección a un nodo o dispositivo. En IPv6, es factible tener más de una dirección asignada a un solo nodo o dispositivo. “Más específicamente, las direcciones IPv6 son asignadas a interfaces, no a nodos”<sup>10</sup>. Por lo que una interface puede tener múltiples direcciones asignadas.

En IPv6 cambian los tipos de direcciones:

- En IPv6 se eliminan las direcciones broadcast, el cual es integrado dentro de multicast.
- En IPv6 se introduce anycast (comunicación uno a uno), como un modo de comunicación, donde, la interfaz de destino puede ser elegida entre varias interfaces. Basándose en el nodo más “cercano” al origen.

---

<sup>10</sup> IPv6 Networking Programming, Jun-ichiro-itojun Hagino. Editorial Elsevier Digital Press Pag.24

## **Capítulo 5. Propuesta de implementación del protocolo IPv6 en la Red Inalámbrica Universitaria.**

Las investigaciones y las pruebas que se han realizado desde el año de 1998, hoy ponen a la Universidad Nacional Autónoma de México listo para dar el siguiente paso, implementar gradualmente el protocolo IPv6 en la RedUNAM.

Dado que la UNAM cuenta con servicios en IPv4 e IPv6, se ha propuesto la tarea de realizar pruebas, con el fin de determinar los requerimientos necesarios para hacer uso del nuevo protocolo.

El principal problema de implementar una solución basada en IPv6 en la RIU, es la falta de documentación por parte del fabricante de los switches controladores, ya que esto, como la gran mayoría de las empresas de telecomunicaciones está en fase de pruebas.

Hasta este punto ya se ha visto los elementos básicos de comunicaciones y de las redes inalámbricas, el funcionamiento y el rol que desempeña el switch controlador y del protocolo IPv6. En este capítulo, se definen los parámetros necesarios para la configuración del switch controlador bajo el protocolo IPv6.

### **5.1.- Definición de configuración.**

El método que se utilizará para realizar las pruebas es el de transición, usando para ello Dual-Stack. Debido a que el controlador no tiene capacidad de enrutar paquetes en IPv6, se optó por usar un router con capacidad en IPv6. Un elemento importante, es la configuración de la red de área local (VLAN). La cual tiene la característica de segmentar o separar de forma lógica el tráfico de una red ayudando en la administración de esta.

Además de usar una Vlan en específico, la cual transportará el tráfico de los usuarios al router con IPv6. También se usaran otras dos Vlan's, las cuales transportaran el tráfico en IPv4 generado por los clientes.

Los switches controladores que están en este momento en producción, tiene la versión 3.4.31, la cual no tiene soporte para IPv6 de forma nativa. Para realizar las pruebas se usará la versión beta 6.1, la cual tiene la capacidad de aceptar direcciones IPv6 en las interfaces.

En el capítulo 3 se definieron los parámetros necesarios para configurar una red inalámbrica. Por lo que primero se debe de iniciar con la configuración de los parámetros de red. El equipo que se usará para realizar las pruebas es un switch controlador Aruba 3400.



## 5.2.- Propuesta de configuración física del switch controlador “Master”

- Interface loopback: La interfaces de loopback permite definir las direcciones en IPv4 y en IPv6.

```
!  
interface loopback  
    ip address 172.16.163.102  
    ipv6 address 2001:1200:200:1::3  
!
```

- Vlan: Para las pruebas se definieron tres Vlan's. La Vlan 98 de administración, la Vlan 100 para el tráfico en IPv4 y la Vlan 500 que enlazara el tráfico hacia la interfaz que está configurada con IPv6

```
vlan 98  
vlan 100  
vlan 500
```

- Interface de la Vlan: La Vlan 98 fue nuestra Vlan de administración, con la cual se puede acceder al equipo de forma remota para realizar cambios en la configuración o monitorear al propio equipo.

```
interface vlan 98  
    ip address 172.16.163.101 255.255.255.0  
  
!  
interface vlan 100  
    ip address 10.1.0.254 255.255.255.0  
  
!  
interface vlan 500  
    ip address 172.16.163.101 255.255.255.0  
    ipv6 address 2001:1200:200:1::2/64  
  
!
```

- Interface física: En la interfaz Gigabit Ethernet 1/0 configuramos la Vlan 98, mientras que en la interfaz 1/2 configuramos los parámetros que nos enlazará con el router en IPv6.

```

interface gigabitethernet 1/0
  description "gig1/0"
  trusted
  trusted vlan 1-4094
  switchport access vlan 98
i
i
interface gigabitethernet 1/2
  description "gig1/0"
  trusted
  trusted vlan 1-4094
  switchport access vlan 500
i

```

- Default-gateway: Para esta configuración se usaran los default-gateway tanto para IPv4 como para IPv6. Con lo cual, los clientes podrán salir a internet por IPv4 así como por IPv6.

```

ip default-gateway 172.16.163.254
ipv6 default-gateway 2001:1200:200:1::1

```

Una vez establecida la configuración, el switch controlador debe ser capaz de comunicarse con ambos Gateways.

Una vez que el equipo sale a red, el siguiente paso es establecer la configuración lógica de la red inalámbrica. El propósito de la configuración es lograr que los clientes una vez que han sido autenticados y asociados, estos puedan salir a internet y acceder a páginas en IPv6, lo cual significa que la configuración es correcta.

### 5.3.- Propuesta de configuración lógica del switch controlador “Master”

Los siguientes puntos son para configurar los parámetros de la red inalámbrica.

- netdestination: Para las pruebas se requieren los segmentos de direcciones 10.1.0.0 y 10.2.0.0, las cuales se les será asignada a los clientes.

```

!
!

```

```
netdestination INTERNAL-NETWORK
  network 10.1.0.0 255.255.0.0
  network 10.2.0.0 255.255.0.0
  !
```

- ip access-list: Para las listas de acceso se crearan tres listas de acceso, una para cada uno de los roles: “Staff”, “Académico” y “Estudiante”, tal y como se usan en la RIU.

```
!
ip access-list session SACL-STAFF
  any any svc-dhcp permit
  user  alias mswitch svc-icmp permit
  user  any udp 68 deny
  user  any udp 161 deny
  user  any udp 162 deny
  user  any svc-dhcp permit
  user  alias mswitch svc-ssh deny
  user  alias mswitch svc-http deny
  user  alias mswitch svc-https deny
  user  any any src-nat pool natpool
!
!
ip access-list session SACL-ACADEMICO
  user  any udp 68 deny
  user  any udp 161 deny
  user  any udp 162 deny
  user  any svc-dhcp permit
  user  alias mswitch svc-ssh deny
  user  alias mswitch svc-http deny
  user  alias mswitch svc-https deny
  user  any any src-nat pool natpool
!
!
ip access-list session SACL-ESTUDIANTE
  user  any udp 68 deny
  user  any udp 161 deny
  user  any udp 162 deny
  user  any svc-dhcp permit
  user  alias mswitch svc-ssh deny
  user  alias mswitch svc-http deny
  user  alias mswitch svc-https deny
  user  any any src-nat pool natpool
  any  any tcp 9100 deny
!
```

- user-role: Para definir los roles se crearan tres roles de usuario, “user-role Staff”, “user-role Académico” y “user-role Staff”, los cuales, contendrán las respectivas listas de acceso previamente definidas.

```
!  
user-role STAFF  
  session-acl SACL-STAFF  
!  
!  
user-role ACADEMICO  
  access-list session SACL-ACADEMICO  
!  
!  
user-role ESTUDIANTE  
  access-list session SACL-ESTUDIANTE  
!
```

- dhcp pool: Esta parte es fundamental, en la cual se le indica a los clientes que red usaran. En una configuración normal, el dhcp pool solo asigna direcciones privadas del segmento netdestination 10.1.0.0.

Para las pruebas realizadas, se requerirán dos pool, el pool de la Vlan100 y el pool de la VLAN500.

```
i  
ip dhcp pool vlan100  
  default-router 10.1.0.254  
  dns-server 172.16.10.2 172.16.204.1  
  domain-name riu.unam.mx  
  lease 0 2 0  
  network 10.1.0.0 255.255.255.0  
  authoritative  
!  
i  
ip dhcp pool vlan500  
  default-router 132.247.209.107  
  dns-server 172.16.10.2 172.16.204.1  
  domain-name riu.unam.mx  
  lease 0 2 0  
  network 10.1.0.0 255.255.255.0  
  authoritative  
!
```

- Perfil de AAA “aaa profile”: En perfil de AAA, será el mismo que actualmente se usa en la RIU, la cual, los usuarios se deben de autenticarse por un servidor Radius.

```
!  
aaa profile "AAP-RIU"  
  initial-role "ESTUDIANTE"  
  authentication-dot1x "default"  
  dot1x-default-role "ESTUDIANTE"  
  dot1x-server-group "SG-RADIUS"  
  radius-accounting "SG-RADIUS"  
!
```

- ssid-profiles: El nombre del SSID que se usará para anunciar la red de prueba fue el de IPV6-RIU.

```
!  
wlan ssid-profile "SSIDP-IPV6-RIU"  
  essid "RIU"  
  opmode wpa-tkip wpa-aes wpa2-aes wpa2-tkip  
!
```

- virtual-ap: Para los virtual-ap o VAP, se definieran para las pruebas, los VAP-DGSCA y el VAP-BC. El VAP de DGSCA se usará para las pruebas con IPv6 y el VAP-BC se asignará para los clientes que usaran IPv4.

```
!  
wlan virtual-ap "VAP-BC"  
  aaa-profile "AAP-RIU"  
  ssid-profile "SSIDP-RIU-WPAMIX"  
  vlan 100  
  no blacklist  
  auth-failure-blacklist-time 0  
!  
!  
wlan virtual-ap "VAP-IPV6"  
  aaa-profile "AAP-RIU"  
  ssid-profile "SSIDP-IPV6-RIU"  
  vlan 500  
  no blacklist  
  auth-failure-blacklist-time 0  
!
```



Cabe hacer mención, que para hacer uso de los VAP que se definieron previamente, se pueden usar de dos formas. EL VAP se puede integrar a un grupo llamado “ap-group” o en un “ap-name”. El ap-group engloba a un conjunto de punto de acceso mientras que un ap-name define a un único punto de acceso.

- ap-group: El VAP-BC se añadirá al interior del grupo “APG-BC”.

```
!  
ap-group "APG-BC"  
  virtual-ap "VAP-BC"  
  ap-system-profile "APSP-LOCAL2"  
!
```

- ap-name: Dentro del ap-name “10.1.1”, el cual identifica al punto de acceso de forma única, se incluirá el VAP de “IPV6”.

```
!  
ap-name "10.1.1"  
  virtual-ap "VAP-IPV6"  
!
```

Una vez ingresada la respectiva información, ya es posible realizar la conexión a la red inalámbrica, la cual estará emitiendo el SSID de la “IPV6-RIU”. Una vez completa la configuración del switch controlador, ahora falta configurar el punto de acceso y la laptop con los parámetros de IPv6.

#### 5.4.- Configuración del punto de acceso.

El punto de acceso que se usará para realizar las pruebas es un punto de acceso Aruba modelo 105, el cual se configurará usando el software hyperTerminal o putty. En el siguiente cuadro se puede observar los parámetros de red necesarios para configurar el punto de acceso.

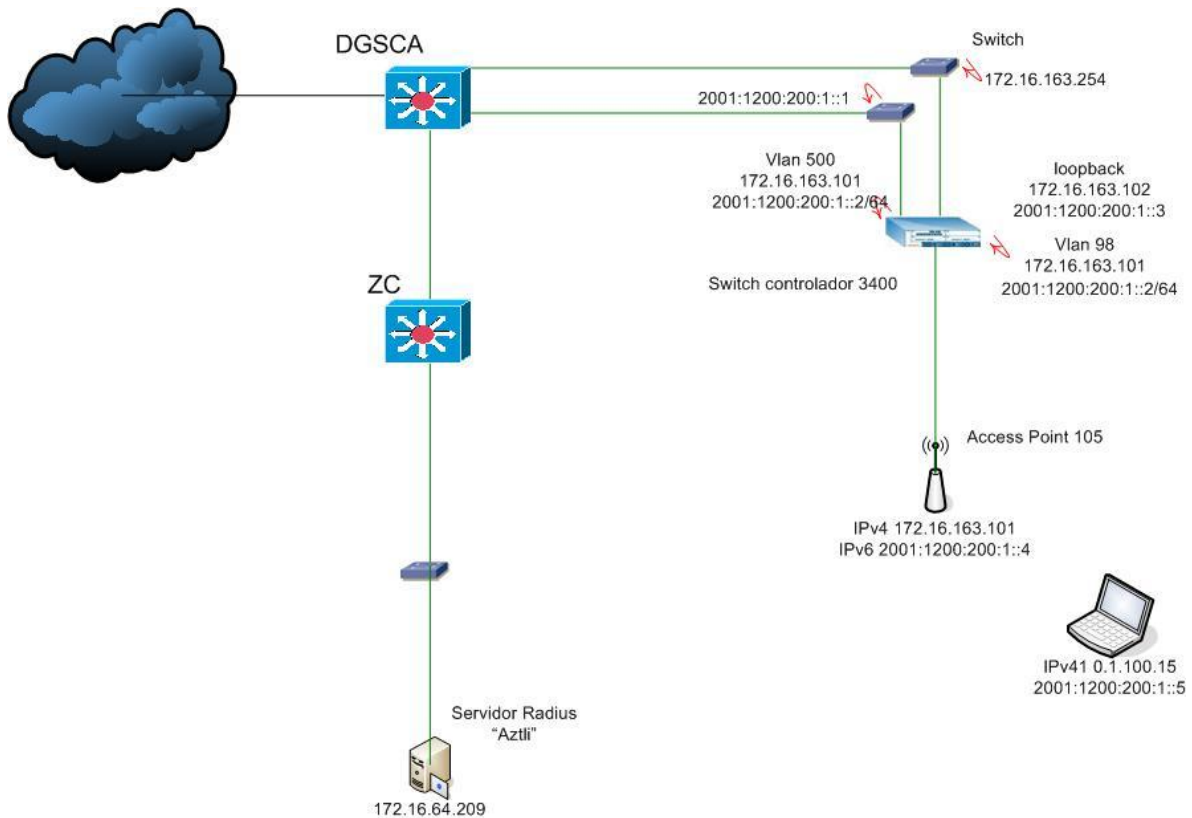
```
apboot>setenv ipaddr 172.16.163.101  
apboot>setenv ip6addr 2001:1200:200:1::4  
apboot>setenv netmask 255.255.255.0
```

```

apboot>setenv gatewayip 172.16.163.254
apboot>setenv gatewayip6 2001:1200:200:1::1
apboot>setenv master 172.16.163.102
apboot>setenv serverip 172.16.163.102
apboot>setenv group APG-IPV6
apboot>setenv name 10.1.1

```

Para tener una mejor visión del propósito de la configuración, en el diagrama 14 se puede observar el diagrama de red propuesto para las pruebas de configuración. En este punto el controlador es capaz de comunicarse con sus respectivos Gateway, lo cual significa que la configuración esta correcta en el aspecto de interconexión.



**Diagrama 14. Distribución de la red de prueba.**

## 5.5.- Prueba de la configuración.

Una vez terminadas las configuraciones físicas como lógicas del switch controlador y del punto de acceso, el siguiente paso es probar la conexión. En este punto, el punto de acceso es capaz de desplegar los SSID “IPV6-RIU” e “IPV6-OPEN” y, finalmente solo quedara por probar que la conexión en IPv6, se esté realizando de forma correcta.

En estos momentos, la mayoría de los sistemas operativos (Ubuntu versión 9.9, Windows Vista y Windows 7) soportan IPv6, en la siguiente imagen se muestra la configuración de la interfaz inalámbrica para el sistema Operativo Windows Vista. Por cuestiones de seguridad no es posible mostrar el direccionamiento, ya que en las pruebas se usaron direcciones validas.

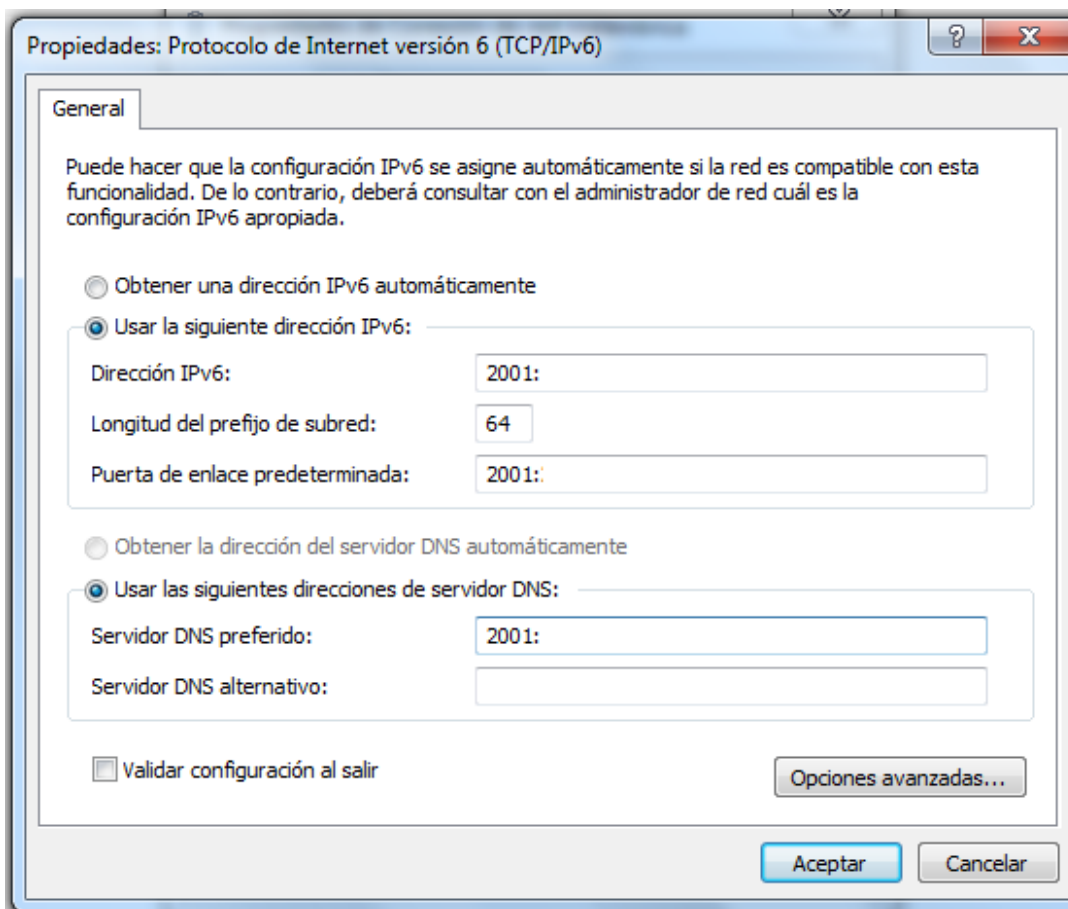


Imagen 2. Configuración de la interfaz inalámbrica con IPv6.

Hay una serie de páginas que sirven para verificar el tipo de conexión que se está realizando. En las pruebas usamos la página [www.kame.net](http://www.kame.net), la cual tiene la peculiaridad de verificar las conexiones realizadas por medio de una imagen dinámica. Si la conexión se realiza por medio de IPv6, mostrara la imagen de una tortuga en movimiento, en caso



contrario, si la tortuga no se mueve esto quiere decir que la conexión se está realizando a través del protocolo IPv4.

Una vez que se ha asignado una dirección IPv6 de forma manual, se puede seguir con el siguiente paso, el cual consiste en asociarse a un SSID, para este caso se usara el SSID, "IPV6-OPEN". Este SSID no nos solicitara ningún parámetro extra de configuración.

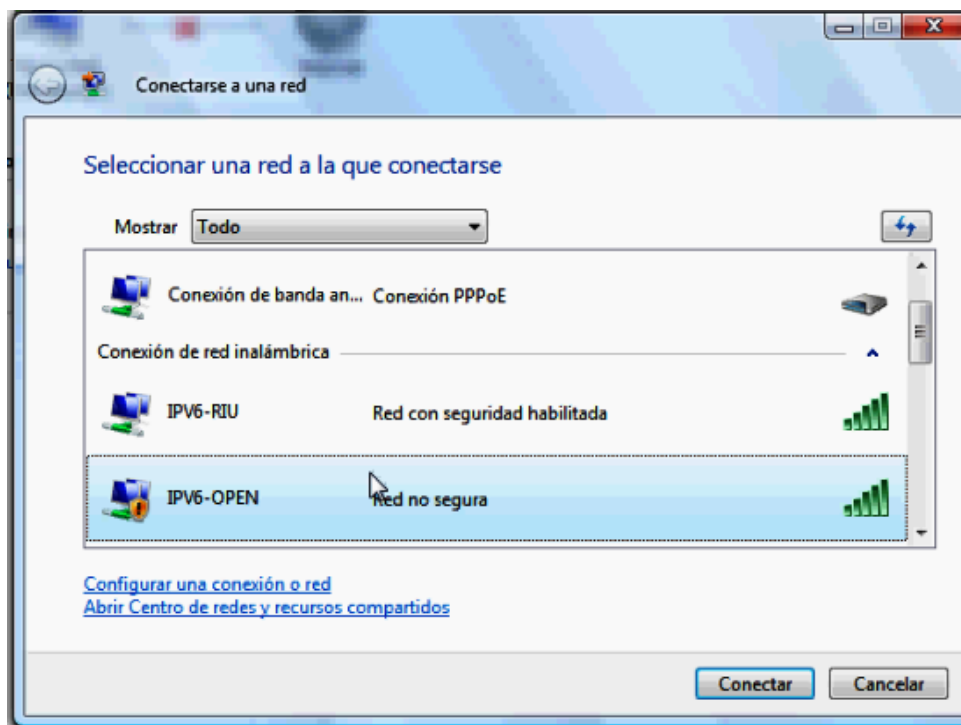


Imagen 3. Redes inalámbricas disponibles.

El controlador nos da la posibilidad de verificar los puntos de acceso que han sido registrados. En la imagen 5 se puede observar el punto de acceso registrado en el controlador

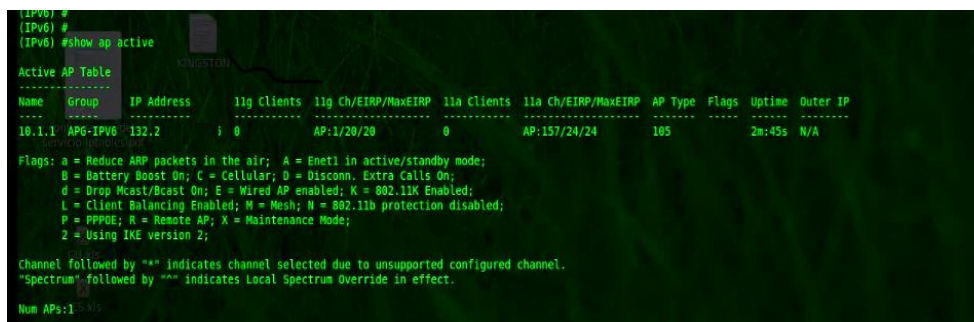


Imagen 4. Punto de acceso registrado en el controlador.

De igual forma, el controlador nos da la posibilidad de verificar los usuarios que han sido asociados al SSID, en la imagen 5 se puede observar que el usuario fue asociado al SSID IPV6-OPEN, y también se puede ver que el usuario le fue asignado el rol de “OPEN”.

IP	Forward mode	Type	MAC	Name	Role	Age(d:h:m)	Auth	VPN link	AP name	Roaming	Essid/Bssid/Phy	Prof
2001:238:200:4...			90:4c:e5:0b:59:69		OPEN	00:00:19			10.1.1	Wireless	IPV6-OPEN/00:24:6c:ab:33:70/g	AAAP
2001:1218:200:1:b1cb:5be0:5bd6:b19		Win Vista	90:4c:e5:0b:59:69		OPEN	00:00:19			10.1.1	Wireless	IPV6-OPEN/00:24:6c:ab:33:70/g	AAAP
fe80::6972:1bac:225e:ab73		Win Vista	90:4c:e5:0b:59:69		OPEN	00:00:19			10.1.1	Wireless	IPV6-OPEN/00:24:6c:ab:33:70/g	AAAP
132.2		Win Vista	90:4c:e5:0b:59:69		OPEN	00:00:19			10.1.1	Wireless	IPV6-OPEN/00:24:6c:ab:33:70/g	AAAP

User Entries: 4/4

Imagen 5. Usuario registrado en el controlador.

## 5.6.- Propuesta de implementación del protocolo IPv6 en la Red Inalámbrica Universitaria (RIU).

La implementación del protocolo IPv6 en la RIU, da pie a iniciar una actualización en la infraestructura de la RedUNAM, ya que de esta depende la conexión de la RIU y de la cual le proporcionará la conectividad en IPv6 tanto en el campus de Ciudad Universitaria, así como hacia las dependencias distribuidas en la Ciudad de México y de los Campus Foráneos.

En el capítulo 3 del presente trabajo, se muestra la tabla 5 con la cantidad de equipos (switches controladores) que conforman actualmente la RIU. En las siguientes imágenes se muestran las ubicación geográficas de las dependencias donde actualmente hay cobertura de la RIU, de esta forma, se tendrá una mejor perspectiva del reto que presenta la implementación del protocolo IPv6.

Actualmente hay cobertura de la RIU en los campus de Juriquilla, Morelia, Cuernavaca, Ensenada y SISAL.

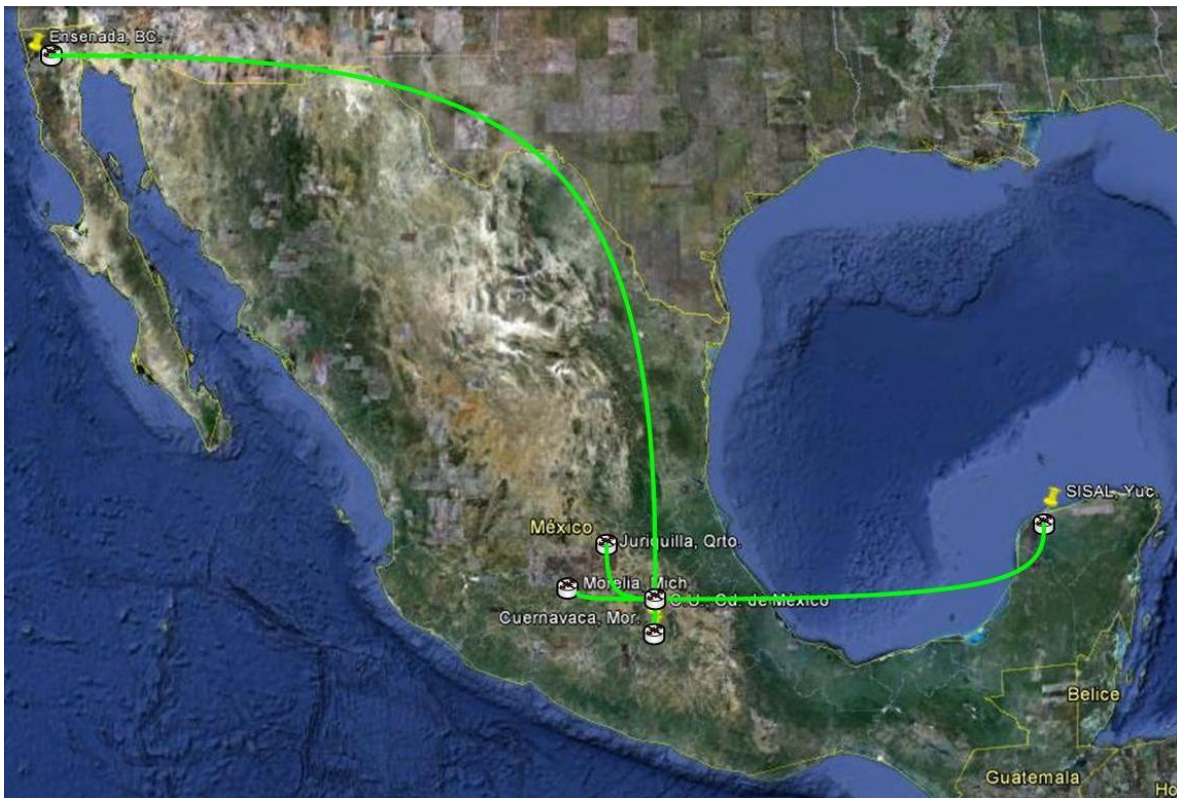


Imagen 6. Distribución de la RIU en campus foráneos.

En la Ciudad de México y el área metropolitana se encuentran las cinco FES y, solo en estas contamos con switches controladores (Locales). Los puntos de acceso que están en las dependencias de la ENAP, ENEO, CUEC y ENM, son administrados desde los switches controladores (Masters) en Ciudad Universitaria.

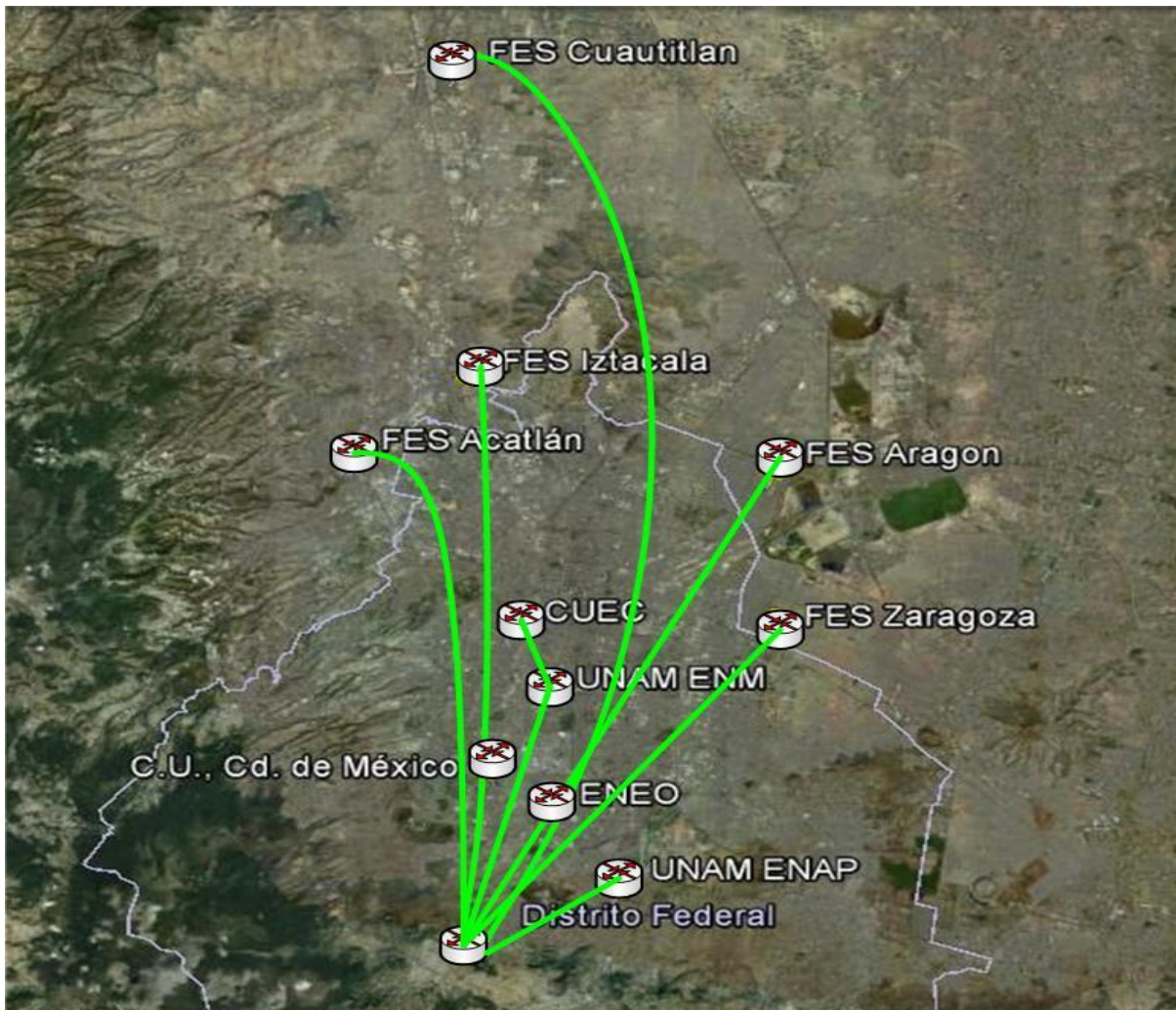


Imagen 7. Distribución de la RIU en el área Metropolitana (FES).

En las preparatorias que están en la Ciudad de México se tiene presencia de la RIU y, solo en el CCH Vallejo se cuenta con un switch controlador (Local).

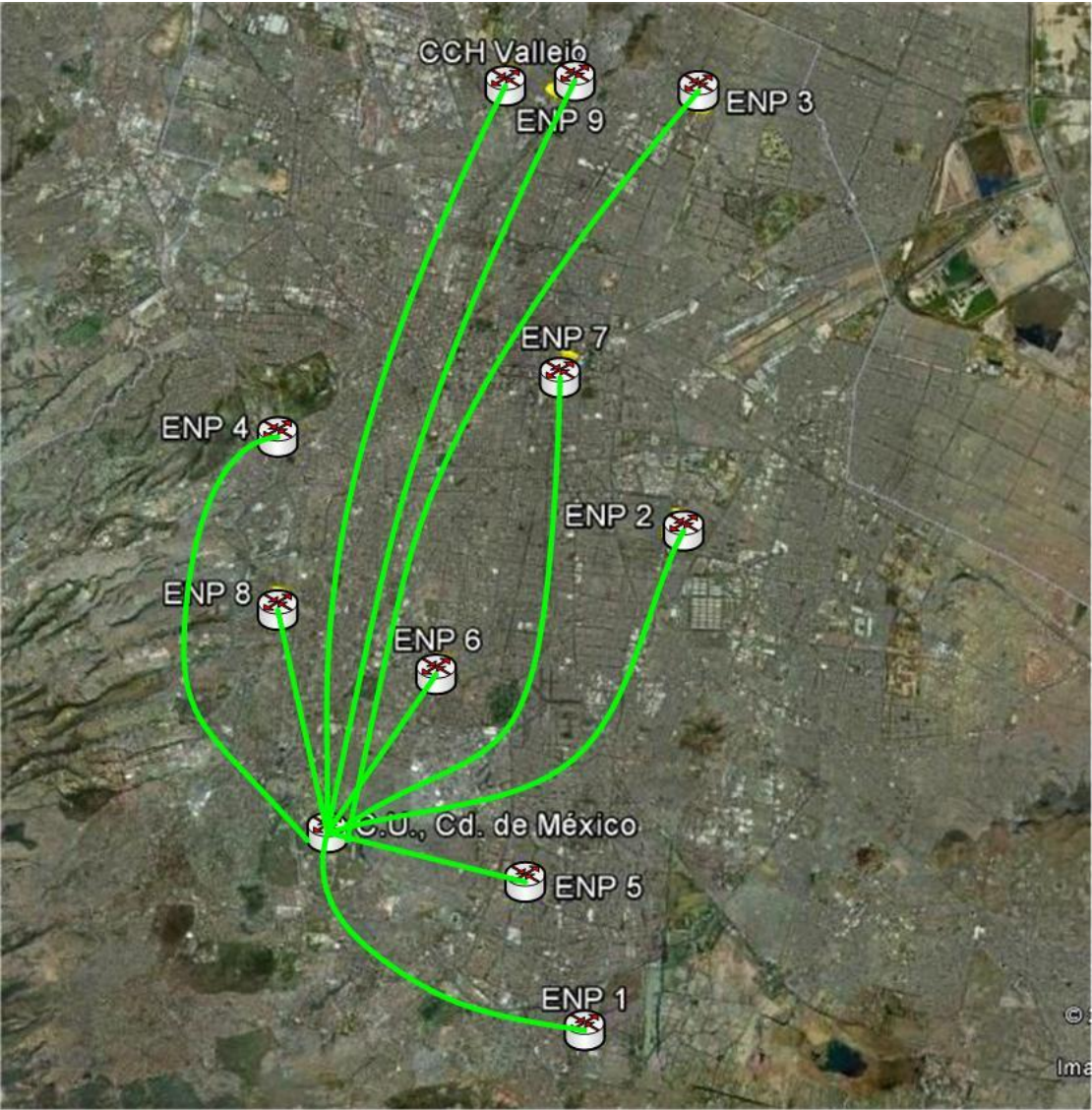


Imagen 8. Distribución de la RIU en el área Metropolitana (ENP).

En Ciudad Universitaria se encuentran los cinco switches controladores (Master) que administran a los demás controladores (Locales).

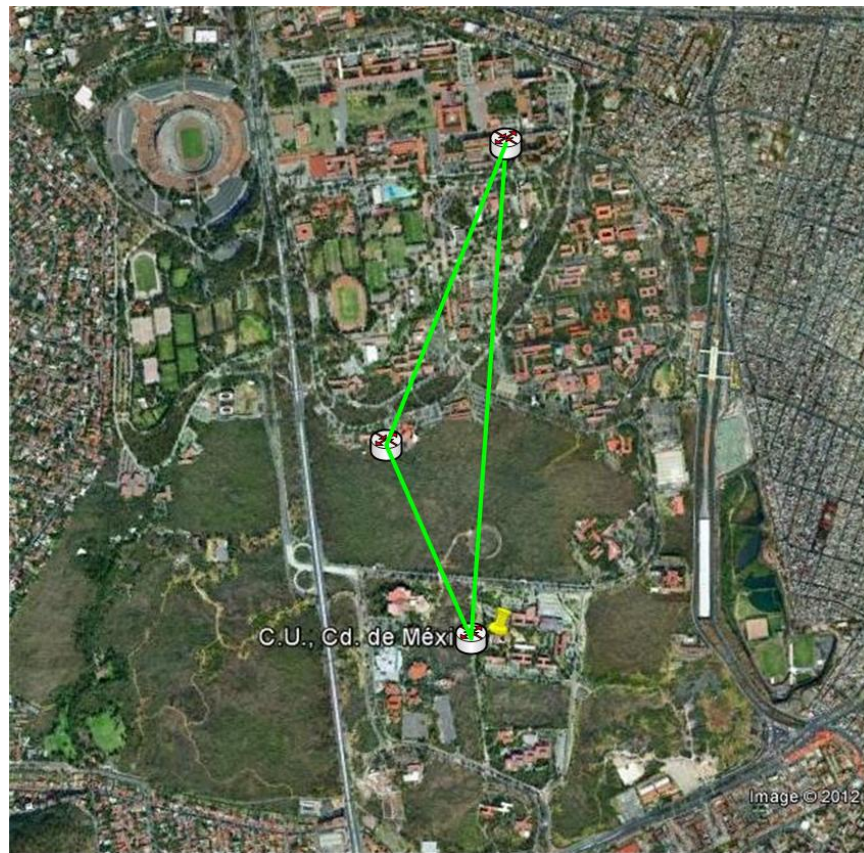


Imagen 9. Distribución de la conexión en CU.

La siguiente tabla muestra una cotización aproximada de los equipos necesarios para implementar el protocolo IPv6 en la RIU de forma general. Actualmente la mayoría de las dependencias: preparatorias, FES y campus foráneos están conectados por router Cisco 2811 y switches 3com.

Propuesta de implementación a IPv6.					
		Switch	Router	Costo SW	Costo Router
Foráneos	Juriquilla, Qro.	1	1	35000	50000
	Morelia, Mich.	1	1	35000	50000
	Cuernavaca, Mor	1	1	35000	50000
	Ensenada, BC.	1	1	35000	50000
	SISAL, Yuc.	1	1	35000	50000
<b>Subtotal</b>		<b>5</b>	<b>5</b>	<b>175000</b>	<b>175000</b>

ENP	ENP1	1	1	30000	45000
	ENP2	1	1	30000	45000
	ENP3	1	1	30000	45000
	ENP4	1	1	30000	45000
	ENP5	1	1	30000	45000
	ENP6	1	1	30000	45000
	ENP7	1	1	30000	45000
	ENP8	1	1	30000	45000
	ENP9	1	1	30000	45000
CCH	CCH Vallejo	1	1	30000	45000
	CCH Azcapotzalco*	1	1	30000	45000
	CCH Oriente*	1	1	30000	45000
	CCH Naucalpan*	1	1	30000	45000
<b>Subtotal</b>		<b>10</b>	<b>10</b>	<b>300000</b>	<b>300000</b>

FES	FES Aragón	1	1	35000	50000
	FES Acatlán	1	1	35000	50000
	FES Iztacala	1	1	35000	50000
	FES Cuautitlán	1	1	35000	50000
	FES Zaragoza	1	1	35000	50000
	ENEO*	1	1	30000	45000
	ENAP*	1	1	30000	45000
	ENM*	1	1	30000	45000
	CUEC*	1	1	30000	45000
<b>Subtotal</b>		<b>9</b>	<b>9</b>	<b>295000</b>	<b>295000</b>

CU	Dependencias CU	4	70	250000	35000
<b>Subtotal</b>		<b>3</b>	<b>70</b>	<b>750000</b>	<b>2450000</b>

<b>Total</b>				<b>1520000**</b>	<b>3220000**</b>
--------------	--	--	--	------------------	------------------

Tabla 8. Estimación del costo para la implementación del protocolo IPv6 en la RIU

\* Dependencias sin switch controlador local.

\*\* Costo de los equipos en dólares.

### 5.6.1.- Ejemplo de implantación del protocolo IPv6 para la FES-Aragón.

Como ejemplo práctico usaremos la FES Aragón, donde actualmente la FES cuenta con 22 puntos de acceso y un switch controlador Local-Aragón. La siguiente imagen muestra el área de cobertura en la FES Aragón.



Imagen 10. Área de cobertura RIU en la FES Aragón.

La implementación del protocolo IPv6 para la FES Aragón, así como en las demás dependencias que lo requieran, deberán actualizar los equipos de telecomunicaciones tanto el router principal como los switches que conforman la red. Ya que, la mayoría de los equipos que conforman la red son equipos que ya sobrepasaron su vida útil.

El router principal debe ser un equipo con alto rendimiento, el cual deberá soportar un incremento en los equipos de computo, así como de los equipos inalámbricos que forman parte de la RIU la cual se incrementa constantemente año con año.

La elección del switch principal o de distribución además de incluir soporte para IPv6 este deberá ser un equipo robusto, con al menos 8 puertos SFP (Small Form-Factor Pluggable) Gigabit Ethernet, ya que, este equipo será el que proporcione la conexión hacia los switches intermedios.

Los switches intermedios o de acceso deberán contar con al menos 24 puertos Ethernet 10/100/1000 Gigabit Ethernet y dos puertos SFP Gigabit Ethernet. La conexión entre el switch de distribución y los switches intermedios se deberán de realizar a través de los

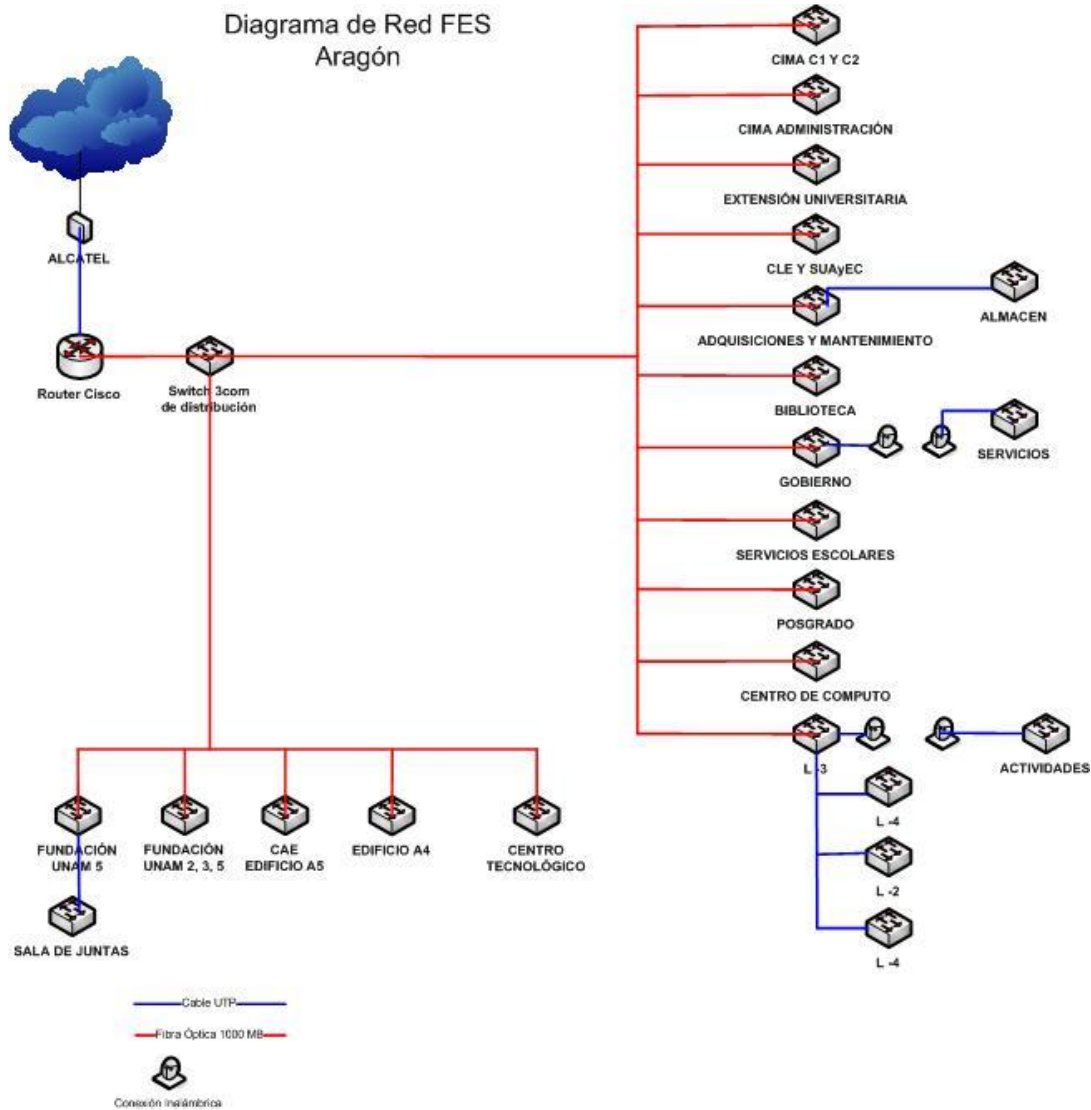


puertos de fibra óptica o SFP. Por lo que hay que considerar el precio de los conectores de fibra ópticas (se debe considerar dos conectores por enlace).

Con la nueva infraestructura se asegura el crecimiento para cualquier red para los próximos 7 o 10 años, dependiendo de la vida útil de los equipos de telecomunicaciones. El beneficio sería inmediato, se incrementaría la velocidad de la LAN, pasando de 10 o 100 Mbps a 1000Mbps.

Los puntos de acceso con el estándar 802.11n incrementarían la velocidad al doble de la actual, pasando de 56 Mbps a un máximo de 300 Mbps. Además, varios de los servicios que ofrece la FES Aragón se verían beneficiados al tener una red más rápida y más eficiente.

El siguiente diagrama muestra la distribución de los equipos de telecomunicaciones, los cuales permitirán contar con IPv6 en toda la red y aumentar la velocidad de 100 Mbps a 1000 Mbps



**Diagrama 15. Propuesta de distribución de equipos de telecomunicaciones para la FES Aragón.**

La siguiente tabla muestra la cantidad de equipos y el costo aproximado en dólares de los equipos necesarios para implementar el protocolo IPv6

		Cantidad	Costo SW	Costo Router
FES Aragón	Router	1	\$5000	\$5000
	Switch “Distribución”	1	\$4000	\$4000
	Switch de “Acceso”	23	\$3000	\$69000
Subtotal				\$78000

**Tabla 9. Total de equipos requeridos para implementar IPv6 en la FES-Aragón.**

Un punto que se debe considerar al momento de actualizar una red, es la actualización del cableado UTP, ya que, la mayoría es de categoría 5e, por lo que es recomendado cambiar al cableado por categoría 6.

Otro punto que no debemos dejar pasar por alto, es la elección de los SFP, ya que, estos se recomiendan que sean de la misma marca que los switches. Se debe considerar un SFP por switch.

En el anexo B se detallan los switches que cuentan con soporte en IPv6 de forma nativa.

## Capítulo 6. Resultados obtenidos.

La propuesta del protocolo IPv6 como se ha visto, lleva más de una década su estudio y el día de hoy se cuenta con bastante literatura informativa del protocolo IPv6, pero, no hay información sobre trabajos o proyectos de la implantación de dicho protocolo y menor aun, sobre la implementación en una solución inalámbrica.

EL trabajo de investigación e implementación se realizo en conjunto con el departamento de Operación de RedUNAM, los cuales nos brindaron su apoyo al ofrecernos los enlaces correspondientes de IPv4 e IPv4.

En este capítulo se mostraran las pruebas realizadas que comprueban nuestros resultados.

### 6.1.- Resultados.

La implementación del protocolo IPv6 en la RIU asegurara principalmente su crecimiento para los próximos años, además de dar a la comunidad universitaria la oportunidad de implementar nuevas herramientas que ayuden a mejorar su desempeño académico.

Cabe hacer mención, que no existe información para llevar a cabo una configuración basada en el protocolo IPv6 por parte del fabricante del equipo. Sin embargo, como se vio en el primer capítulo, el protocolo IPv4 como el protocolo IPv6 son direcciones lógicas a diferencia de las direcciones físicas (direcciones MAC). Por lo que nuestro trabajo se centro en la configuración y adaptación de dicho protocolo en las respectivas interfaces que permiten establecer la comunicación con el exterior.

Los resultados están divididos en dos partes:

- **Comprobación de conexión de red con IPv6:** Esta etapa está enfocada a comprobar que la conexión con el protocolo IPv6 se realice de correcta entre el switch controlador y el router que funge como puerta de enlace o Gateway.
- **Configuración inalámbrica:** En esta etapa está enfocada a comprobar que los parámetros actuales sean asignados de forma normal (perfiles de usuarios: Staff, Académico y Estudiante), lo cual nos da la certeza que una migración es factible sin mayores cambios en la configuración actual.

## 6.2.- Comprobación de conexión de red con IPv6.

Una vez configuradas los parámetros de red en las interfaces contamos con la herramienta ping, la cual nos ayuda a verificar la conexión entre dos puntos.

Para comprobar que la conexión con el router o gateway se ha establecido de forma adecuado, se puede usar la herramienta ping, la cual comprueba el estado de la conexión. Para realizar un ping a una dirección en IPv6 desde el switch controlador, se cuenta con herramienta *ping ipv6* (ping -6 para sistema operativo Windows y ping6 en Linux).

En el siguiente cuadro, se puede observar la prueba del ping para comprobar la conectividad desde nuestro switch controlador en IPv6, hacia su respectivo default gateway que se configuro en el capítulo 5. El equipo tiene su propia herramienta incorporada para este caso, en el siguiente cuadro se muestra el comando usado, así como la respuesta de éxito que el gateway envía al switch controlador.

```
(IPv6) #ping ipv6 2001:1200:200:1::1

Press 'q' to abort.

Sending 5, 100-byte ICMP Echos to
2001:1200:200:1::1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip
min/avg/max = 0.558/4.558/20.465 ms
```

Una vez que se ha establecido la comunicación con el gateway, el switch será capaz de enviar tráfico en IPv6. También se realizo las pruebas para verificar la conexión con el default gateway, pero para la dirección en IPv4.

```
(IPv6) #ping 172.16.1.1

Press 'q' to abort.

Sending 5, 100-byte ICMP Echos to
2001:1200:200:1::1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip
min/avg/max = 1./4.558/20.465 ms
```

De esta forma podemos asegurar que se ha establecido la conexión. La conexión hacia la interfaz del router, es por la cual el tráfico saldrá hacia otro segmento de red o hacia Internet.

La segunda prueba consistió en realizar una consulta a la página [www.kame.net](http://www.kame.net), para lograr esto, primero el usuario debió ser asociado y después autenticado para establecer una sesión en la red de prueba. Con la configuración que se determino, es posible para cualquier perfil; ya sea “STAFF”, “ACADEMICO” o “ESTUDIANTE” establecer una conexión por IPv6. En la imagen 4 se muestra la página [www.kame.net](http://www.kame.net). Al momento de acceder a dicha pagina se logra ver la imagen de la tortuga en movimiento, lo cual indica que la conexión se estableció en IPv6.

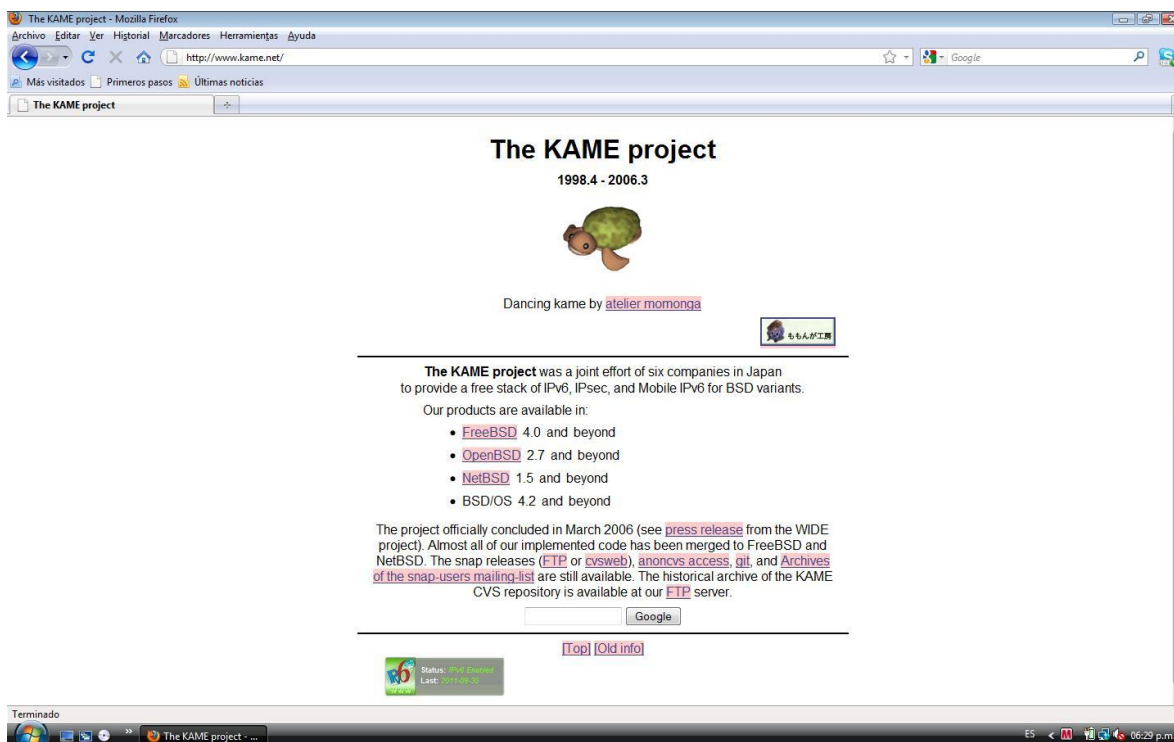


Imagen 11. Pagina [www.kame.net](http://www.kame.net), con acceso en IPv6.

También realizamos una consulta a una página en IPv6, para ello usamos la propia dirección IPv6 del controlador. Para acceder a una página desde el explorador, la dirección se debe de escribir entre corchetes.

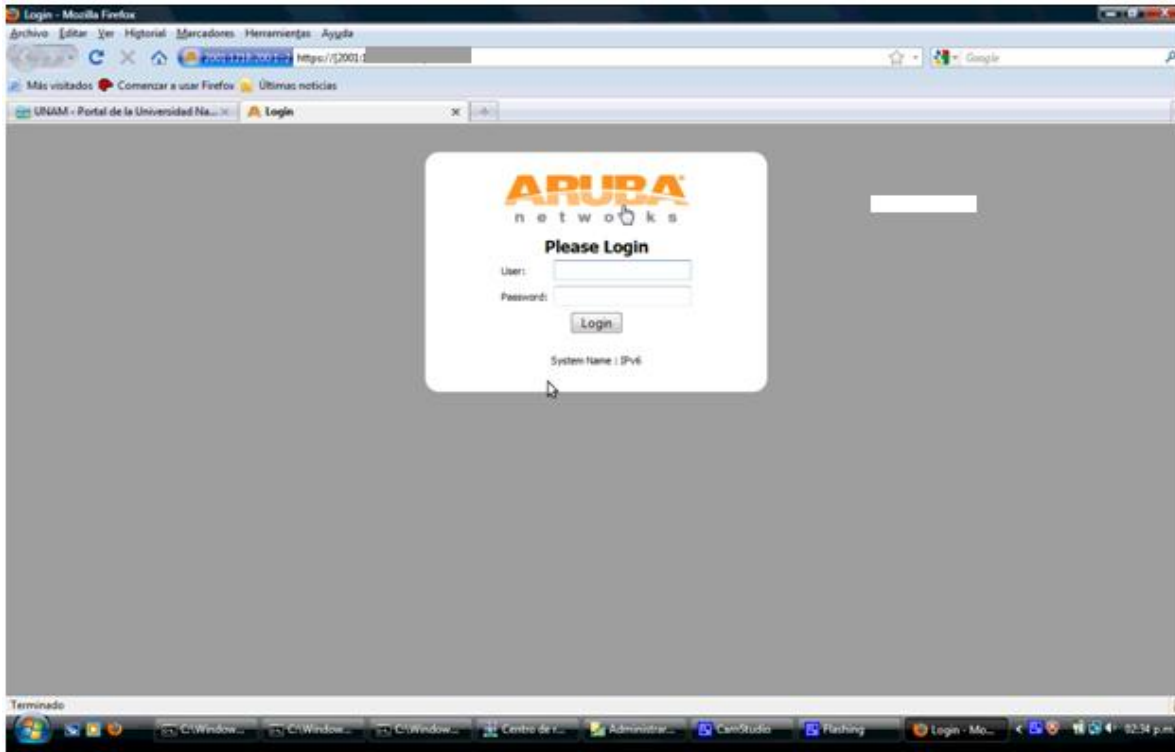


Imagen 12. Para acceder al controlador [https://\[2001:1266:1::6\]:4343](https://[2001:1266:1::6]:4343)

## Conclusiones.

Del presente trabajo se puede concluir que:

Las pruebas que realizamos fueron exitosas, esto se debe en primer lugar, a la red donde llevamos a cabo nuestras pruebas. Los router tiene la capacidad de soportar el protocolo IPv6 de forma nativa. En el diagrama 14 del capítulo 5, podemos ver donde se encuentra implementada la red de pruebas dentro de la RedUNAM.

Sin embargo, para llevar a cabo la implementación del protocolo IPv6 en la RIU, la infraestructura actualmente no tiene la capacidad de soportar tal tarea. Principalmente a que la mayoría de los router que dependen los switches controladores no tienen soporte para IPv6, estos deben ser actualizados o en su defecto ser cambiados por equipos nuevos. Como se observo en los diagramas 1 y 2 del capítulo 3, hay una gran cantidad de equipos intermedios de los cuales depende los switches controladores, por lo que la implementación será llevada a cabo paulatinamente debido a los costos de los equipos.

Otro punto a considerar es la versión, como habíamos comentado los switches controladores tiene la versión 3.4.1 y la versión que ocupamos para realizar las pruebas fue con la versión 6.1 la cual es una versión beta. La cual, primero debe pasar una serie de revisiones para llegar a estar lista para su comercialización, por lo que, nuevos aspectos en la configuración llegarían a cambiar.

La implementación de una red completamente en IPv6 ya es posible, pero, el mayor el problema en estos momentos son los costos tan elevados. En primera instancia, hay que considerar el costo de los equipos de telecomunicaciones. La mayoría de los equipos actuales, principalmente router no soportan la actualización del su sistema operativo para soportar IPv6.

Otro punto importante que no debemos pasar por alto, es la conexión que nos proporciones nuestro proveedor de Internet, el costo de un enlace en IPv6 es escaso y a precio elevado. Si consideramos que un enlace (E1) está alrededor de unos 25 a 35 mil pesos, ahora un enlace en IPv6 el costo se incrementa al doble (50 a 70 mil pesos).



## **Expectativas**

El principal beneficio de cualquier red que implemente el protocolo IPv6, asegurará su crecimiento de forma sustentable para los próximos años. Pero hay que considerar nuevas cuestiones.

Las direcciones IPv6 son tan vastas que nos tocaría de al menos 2 o 5 direcciones por habitante en la tierra, tendríamos nuestra propia dirección IP, tal como el día de hoy tenemos nuestro número telefónico. Probablemente se asocie nuestro número telefónico con nuestra dirección IP, para tener voz sobre IP o VoIP, la cual es más barata que la telefonía tradicional.

Con la capacidad de los equipos portátiles nuestros dispositivos se volverían en potentes servidores, podríamos crear, guardar y transmitir contenido en línea. Nuestros dispositivos portátiles se convertirían en nuestras nubes personales.

En la RIU se podrían proporcionar servicios adicionales a la comunidad universitaria, como sería VoIP,

El sábado, 10 de diciembre de 2011, se percibió un temblor en la Ciudad de México con magnitud de 6.5 grados en la escala de Richter. El evento presento un caso muy particular, la red telefónica convencional como la de celular se colapso durante más de una hora. El único servicio que estuvo disponible fue, la red de datos, tanto los módems como los teléfonos celulares con conexión de datos conservaban su conexión.

Este hecho, demuestra que la telefonía sobre datos o VoIP, presenta mayor estabilidad y disponibilidad. Esto demuestra que el telefonía sobre IP, esta lista para una muy posible migración una vez que el protocolo IPv6 este en operación a nivel nacional.

## **Discusiones.**

La implementación del protocolo IPv6 en la RIU o en cualquier red, ya sea casera o de una gran empresa, nos traerá nuevos temas a discutir.

En primera instancia, todas las direcciones IPv6 son validas o públicas, lo que quiere decir, que cualquier dirección IPv6 usada por cualquier dispositivo será ruteada a través de Internet, caso contrario a las direcciones IPv4, donde las direcciones de carácter privadas o no homologadas no pueden ser ruteadas hacia Internet.

Por propósitos de administración, prácticos y de seguridad, el uso de las direcciones privadas otorga cierto control sobre los servicios que nos proporciona una red, por ejemplo (servidores Web, de correo, de FTP etc.). Con la implementación de IPv6, cualquier usuario podrá convertir su dispositivo en un servidor. En la RIU tenemos la posibilidad de crear políticas de asignación a través de los perfiles con los que contamos actualmente.

Como hemos visto, la configuración de la RIU nos permite hacer configuraciones específicas, de acuerdo a los requerimientos y necesidades de nuestros usuarios. Podemos crearles redes para sus eventos (nombres de red personalizados, seguridad por medio de una clave única o de acceso libre), dicha configuración la podemos implementar a través de diversas maneras:

- A todos los usuarios de la RIU, sin la distinción de perfiles.
- A una facultad, instituto o dependencia de la UNAM.
- A un grupo específico de puntos de acceso.
- A un punto de acceso en específico.

El presente trabajo, es una muestra de los alcances que nos ofrece el protocolo IPv6 en los procesos de administración y control del lado del administrador y sus alcances serán reflejados en el usuario final.

Así mismo, concluyo que los alcances de dicho protocolo no han sido explotados al 100%, esperando que el presente trabajo sea una guía para contribuir al conocimiento de nuestra sociedad.

## Anexos A. Publicaciones referente a fechas sobre pruebas al protocolo IPv6.

Artículo Publicado el 8 de junio del 2011, en el diario de circulación nacional El Universal.

Nombre del artículo: A prueba, el nuevo protocolo de internet.

Tomado de: <http://www.eluniversal.com.mx/articulos/64462.html>

Escrito por: eca

### A prueba, el nuevo protocolo de internet

En el World IPv6 Day, el mundo realiza un ensayo general sobre la transición al nuevo sistema de acceso a la web

Miércoles 08 de junio de 2011  
GDA/El País/Uruguay | El Universal  
09:00

[Comenta la Nota](#)



Hoy se realiza un experimento en todo el mundo para testear el nuevo protocolo de la web. Google, Yahoo! y Facebook, entre otras grandes compañías ofrecerán sus contenidos en IPv6 para que se realice una transición masiva.



Share

El objetivo de la prueba que tiene lugar hoy es medir el funcionamiento del nuevo sistema en grandes empresas y certificar si están preparadas para el cambio. Los usuarios no sentirán modificaciones en el servicio. El ensayo durará 24 horas y se hará en todo el planeta.

Hoy se celebra el World IPv6 Day, algo parecido a ensayo general promovido por la Internet Society (ISOC) para preparar la transición al nuevo protocolo de acceso a Internet.

Las principales organizaciones y compañías de Internet se han unido para realizar éste, el mayor experimento global sobre la nueva tecnología de Internet: el World IPv6 Day. Se trata de un ensayo mundial en el que se hará una prueba masiva durante 24 horas sobre el funcionamiento del nuevo protocolo de Internet.

El World IPv6 Day busca motivar a las principales empresas de la industria de Internet, incluyendo proveedores de servicios, fabricantes de equipos, proveedores de sistemas operativos y empresas de contenido, a preparar sus servicios en IPv6 para asegurar una transición exitosa para cuando las direcciones IPv4 se agoten de forma definitiva.

La iniciativa es coordinada por The Internet Society (ISOC) y en la región cuenta con el respaldo del Registro de Direcciones de Internet para América Latina y el Caribe (Lacnic).

Durante el día de hoy gigantes de la red, como Facebook, Google, Yahoo!, Bing (el buscador de Microsoft), Akamai (brinda una cuarta parte de todo el tráfico mundial de Internet) y Limelight Networks, entre otras grandes compañías, ofrecerán sus contenidos en IPv6 para una prueba de 24 horas.

La gran mayoría de los usuarios podrán acceder a los servicios como de costumbre, pero en casos excepcionales, una mala configuración o equipos de red con problemas, pueden afectar el acceso a sitios web que participen en la prueba.

El explosivo desarrollo de Internet ha generado una gran demanda de los bloques disponibles de direcciones IP -un número único asignado a un dispositivo informático conectado a una red- lo que obligó a crear un nuevo protocolo para permitir la expansión de la red de redes.

El sistema más utilizado actualmente, IPv4, tiene un número finito de direcciones IP, con más de 4 mil millones de combinaciones posibles, que hoy se han agotado. Para sustituirlo se ideó IPv6, un protocolo mucho más avanzado y amplio, con mayores posibilidades.

IPv6 es la nueva generación del protocolo de Internet y es esencial para hacer que Internet siga creciendo en las próximas décadas.

eca



El IPv6 es un protocolo mucho más avanzado y amplio, con mayores posibilidades para Internet (Foto: Especial)



#### Notas Relacionadas

[La esperanza está en el IPv6](#) 2011-06-08

[Se agotan las direcciones IP ¿y ahora?](#) 2011-06-08

Artículo Publicado el 18 de enero de 2012, en el diario de circulación nacional El Universal.

Nombre del artículo: Gigantes de Internet alistan cambio al IPv6

Tomado de: <http://www.eluniversal.com.mx/articulos/68520.html>

Escrito por: eca

# Gigantes de internet alistan cambio al IPv6


Los sitios usarán nuevos 'números telefónicos' a partir de junio para conectar a los usuarios con los sitios web

Miércoles 18 de enero de 2012

AP | El Universal

09:18

[Comenta la Nota](#)

 GINEBRA.- Las gigantes de la Internet, incluidas Yahoo, Facebook y AT&T, comenzarán a usar un nuevo sistema de direcciones numéricas para conectar a los usuarios con los sitios web a partir del 6 de junio.



Una alianza de grandes compañías tecnológicas informó el martes que sigue adelante con sus planes de desplegar permanentemente nuevos "números telefónicos" para los dispositivos conectados a Internet, tras realizar con éxito una prueba en junio pasado.

Los Ingenieros consideran que el nuevo sistema, conocido como IPv6, es necesario, porque el crecimiento incesante de la Internet implica que la vieja forma de asignar direcciones en línea ha llegado prácticamente a su límite.

Fabricantes de equipo, como Cisco y D-Link, participan también en el lanzamiento, que hará posibles a la postre más de 340 billones de billones de billones de direcciones de Internet.

eca



El nuevo sistema hará posibles a la postre más de 340 billones de billones de billones de direcciones de Internet. (Foto: Especial)



## Anexos B. Guías técnica de switches con soporte en IPv6.

Fabricante: HP

Nombre del artículo: Guía técnica de switches HP 38000

Tomado de: <http://h17007.www1.hp.com/es/es/products/switches/index.aspx>

# QuickSpecs

HP 3800 Switch Series

## Overview

### Models

HP 3800-24G-PoE+-25FP+ Switch	J9573A
HP 3800-48G-PoE+-40FP+ Switch	J9574A
HP 3800-24G-25FP+ Switch	J9575A
HP 3800-48G-40FP+ Switch	J9576A
HP 3800-24G-2XG Switch	J9585A
HP 3800-48G-4XG Switch	J9586A
HP 3800-24G-PoE+-2XG Switch	J9587A
HP 3800-48G-PoE+-4XG Switch	J9588A
HP 3800-245FP-25FP+ Switch	J9584A

### Key features

- Fully-managed layer 3 stackable switch series
- Low-latency, highly resilient architecture
- SFP+, 10GBase-T, PoE+, modular stacking
- HP FlexChassis-Mesh - stack up to 10 switches
- Industry leading lifetime warranty

### Product overview

The HP 3800 Switch Series is a family of fully managed Gigabit Ethernet switches. There are a total of nine switch models—a 24-port switch, a 48-port switch, a 24-port PoE+ switch, a 48-port PoE+ switch with either SFP+ or 10GBASE-T uplinks, and a 24-port SFP switch with 2 SFP+ uplinks. HP 3800 Series Switches utilize the latest HP ProVision ASIC technology and combine the latest advances in hardware engineering to deliver one of the most resilient and energy-efficient switches in the industry. The 3800 series implements meshed stacking technology to deliver chassis-like resiliency in a flexible stackable form factor.

### Features and benefits

#### Quality of Service (QoS)

- **Layer 4 prioritization:** enables prioritization based on TCP/UDP port numbers
- **Class of Service (CoS):** sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
- **Bandwidth shaping:**
  - Port-based rate limiting: provides per-port ingress-/egress-enforced maximum bandwidth
  - Classifier-based rate limiting: uses an access control list (ACL) to enforce maximum bandwidth for ingress traffic on each port
  - Guaranteed minimum: provides per-port, per-queue egress-based guaranteed minimum bandwidth
- **Advanced classifier-based QoS:** classifies traffic using multiple match criteria based on Layer 2, 3, and 4 information; applies QoS policies such as setting priority level and rate limit to selected traffic on a per-port or per-VLAN basis
- **Remote Intelligent Mirroring:** mirrors selected ingress/egress traffic based on ACL, port, MAC address, or VLAN to a local or remote HP 8200 zl, 6600, 6200 yl, 5400 zl, 3800, or 3500 switch anywhere on the network
- **RMON, XRMON, and sFlow v5:** provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events
- **Traffic prioritization:** allows real-time traffic classification into eight priority levels mapped to eight queues



# QuickSpecs

HP 3800 Switch Series

## Overview

### Models

HP 3800-24G-PoE+-2SFP+ Switch	J9573A
HP 3800-48G-PoE+-4SFP+ Switch	J9574A
HP 3800-24G-2SFP+ Switch	J9575A
HP 3800-48G-4SFP+ Switch	J9576A
HP 3800-24G-2XG Switch	J9585A
HP 3800-48G-4XG Switch	J9586A
HP 3800-24G-PoE+-2XG Switch	J9587A
HP 3800-48G-PoE+-4XG Switch	J9588A
HP 3800-24SFP-2SFP+ Switch	J9584A

### Key features

- Fully-managed layer 3 stackable switch series
- Low-latency, highly resilient architecture
- SFP+, 10GBase-T, PoE+, modular stacking
- HP FlexChassis-Mesh - stack up to 10 switches
- Industry leading lifetime warranty

### Product overview

The HP 3800 Switch Series is a family of fully managed Gigabit Ethernet switches. There are a total of nine switch models—a 24-port switch, a 48-port switch, a 24-port PoE+ switch, a 48-port PoE+ switch with either SFP+ or 10GBASE-T uplinks, and a 24-port SFP switch with 2 SFP+ uplinks. HP 3800 Series Switches utilize the latest HP ProVision ASIC technology and combine the latest advances in hardware engineering to deliver one of the most resilient and energy-efficient switches in the industry. The 3800 series implements meshed stacking technology to deliver chassis-like resiliency in a flexible stackable form factor.

### Features and benefits

#### Quality of Service (QoS)

- **Layer 4 prioritization:** enables prioritization based on TCP/UDP port numbers
- **Class of Service (CoS):** sets the IEEE 802.1p priority tag based on IP address, IP Type of Service (ToS), Layer 3 protocol, TCP/UDP port number, source port, and DiffServ
- **Bandwidth shaping:**
  - Port-based rate limiting: provides per-port ingress-/egress-enforced maximum bandwidth
  - Classifier-based rate limiting: uses an access control list (ACL) to enforce maximum bandwidth for ingress traffic on each port
  - Guaranteed minimum: provides per-port, per-queue egress-based guaranteed minimum bandwidth
- **Advanced classifier-based QoS:** classifies traffic using multiple match criteria based on Layer 2, 3, and 4 information; applies QoS policies such as setting priority level and rate limit to selected traffic on a per-port or per-VLAN basis
- **Remote Intelligent Mirroring:** mirrors selected ingress/egress traffic based on ACL, port, MAC address, or VLAN to a local or remote HP 8200 zl, 6600, 6200 yl, 5400 zl, 3800, or 3500 switch anywhere on the network
- **RMON, XRMON, and sFlow v5:** provide advanced monitoring and reporting capabilities for statistics, history, alarms, and events
- **Traffic prioritization:** allows real-time traffic classification into eight priority levels mapped to eight queues



Fabricante: Cisco System

Nombre del artículo: Guía técnica de Switch Catalyst 3760

Tomado de: <http://www.cisco.com/web/MX/index.html>



Data Sheet

## Cisco Catalyst 3750-X and 3560-X Series Switches

The Cisco® Catalyst® 3750-X and 3560-X Series Switches are an enterprise-class lines of stackable and standalone switches, respectively. These switches provide high availability, scalability, security, energy efficiency, and ease of operation with innovative features such as Cisco StackPower (available only on the Catalyst 3750-X), IEEE 802.3at Power over Ethernet Plus (PoE+) configurations, optional network modules, redundant power supplies, and Media Access Control Security (MACsec) features. The Cisco Catalyst 3750-X Series with StackWise® Plus technology provides scalability, ease of management and investment protection for the evolving business needs. The Cisco Catalyst 3750-X and 3560-X enhance productivity by enabling applications such as IP telephony, wireless, and video for borderless network experience.

Cisco Catalyst 3750-X and 3560-X Series primary features:

- 24 and 48 10/100/1000 PoE+, non-PoE models, and 12 and 24 GE SFP port models
- Four optional uplink network modules with GE or 10GE ports
- Industry first PoE+ with 30W power on all ports in 1 rack unit (RU) form factor
- Dual redundant, modular power supplies and fans
- Media Access Control Security (MACsec) hardware-based encryption
- Flexible NetFlow and switch-to-switch hardware encryption with the uplink Service Module
- Open Shortest Path First (OSPF) for routed access in IP Base image
- IPv4 and IPv6 routing, Multicast routing, advanced quality of service (QoS), and security features in hardware
- Enhanced limited lifetime warranty (LLW) with next business day (NBD) advance hardware replacement and 90 day access to Cisco Technical Assistance Center (TAC) support
- Enhanced Cisco EnergyWise for operational cost optimization by measuring actual power consumption of the PoE devices, reporting, and reducing energy consumption across the network
- USB Type-A and Type-B ports for storage and console respectively and an out-of-band Ethernet management port

In addition to the above features, the Cisco Catalyst 3750-X switches also offer:

- Cisco StackPower™ technology: An innovative feature and industry first for sharing power among stack members
- Cisco StackWise Plus technology for ease of use and resiliency with 64 Gbps of throughput
- Investment protection with backward compatibility with all other models of Cisco Catalyst 3750 Series Switches

## Standalone Switches

Figure 2 shows Cisco Catalyst 3560-X Series Switches.

Figure 2. Cisco Catalyst 3560-X Series Switches



Table 2 shows the Cisco Catalyst 3560-X Series configurations.

Table 2. Cisco Catalyst 3560-X Series Configurations

Feature Set	Models	Total 10/100/1000 Ethernet Ports	Default AC Power Supply	Available PoE Power
LAN Base	WS-C3560X-24T-L	24	350W	-
	WS-C3560X-48T-L	48		
	WS-C3560X-24P-L	24 PoE+	715W	435W
	WS-C3560X-48P-L	48 PoE+		
	WS-C3560X-48PF-L	48 PoE+	1100W	800W
IP Base	WS-C3560X-24T-S	24	350W	-
	WS-C3560X-48T-S	48		
	WS-C3560X-24P-S	24 PoE+	715W	435W
	WS-C3560X-48P-S	48 PoE+		
	WS-C3560X-48PF-S	48 PoE+	1100W	800W

## Cisco Catalyst 3750-X and 3560-X Series Software

In addition to IP Base and IP Services feature sets, the Cisco Catalyst 3750-X and 3560-X Series come with a new LAN Base feature set. The three feature sets available with all Cisco Catalyst 3750-X and 3560-X Series switches are:

- LAN Base: Enhanced Intelligent Services
- IP Base: Baseline Enterprise Services
- IP Services: Enterprise Services

The LAN Base feature set offers enhanced intelligent services that includes comprehensive Layer 2 features, with up-to 255 VLANs. The IP Base feature set provides baseline enterprise services in addition to all LAN Base features, with 1K VLANs. IP Base also includes the support for routed access, StackPower (available only on the Catalyst 3750-X), MACsec, and the new Cisco Service Module. The IP Services feature set provides full enterprise services that includes advanced Layer 3 features such as Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Protocol Independent Multicast (PIM), and IPv6 routing such as OSPFv3 and EIGRPv6. All software feature sets support advanced security, QoS, and management features.



Fabricante: Brocade

Nombre del artículo: Guía técnica de switches Brocade ICX 6610

Tomado de: <http://www.brocade.com/products/all/switches/index.page>

DATA SHEET

www.brocade.com

# BROCADE ICX 6610 SWITCH

## ENTERPRISE LAN SWITCHING

## Chassis-Like Capabilities in a Stackable Form Factor

### HIGHLIGHTS

- Delivers chassis-level performance and availability, providing an optimal user experience for streaming video, VDI, UC, and other critical applications
- Offers unprecedented stacking performance with 320 Gbps of stacking bandwidth, eliminating inter-switch bottlenecks
- Provides up to 1 Tbps of total switching capacity with up to 384 1 GbE and 64 10 GbE per stack for campus network edge and aggregation layers
- Provides unmatched availability with four redundant 40 Gbps stacking ports per switch, hitless stacking failover, hot switch replacement, and dual hot-swappable power supplies and fans
- Simplifies network operations and protects investments with Brocade HyperEdge™ technology\*, enabling single-point network lifecycle management and advanced services sharing across a heterogeneous stack

The Brocade One™ strategy helps simplify networking infrastructures through innovative technologies and solutions. The Brocade ICX 6610 Switch supports this strategy by enabling non-stop network access to today's mission-critical applications with the best price/performance while ensuring scalability for tomorrow's needs.

Today's enterprise campus networks are expected to deliver services thought impossible just a few years ago. High-Definition (HD) video conferencing, real-time collaboration, Unified Communications (UC), and Virtual Desktop Infrastructure (VDI) are only a few of the applications that organizations are deploying to enhance employee productivity, improve customer service, and create a competitive advantage. These same networks must also provide anytime, anywhere mobile access and scale to meet rising user expectations. At the same time, organizations face continued pressure to reduce costs and do more with less. More than ever, campus networks need to quickly and efficiently evolve with the ever-changing business environment.

### COMBINING THE BEST OF A CHASSIS AND A STACKABLE SWITCH

The Brocade® ICX® 6610 Switch redefines the economics of enterprise networking by providing unprecedented levels of performance, availability, and flexibility in a stackable form factor—delivering the capabilities of a chassis with the flexibility and cost-effectiveness of a stackable switch.

### Class-Leading Performance for Today and Tomorrow

The Brocade ICX 6610 delivers wire-speed, non-blocking performance across all ports to support latency-sensitive applications such as real-time voice and video streaming and VDI. Brocade ICX 6610 Switches can be stacked using four full-duplex 40 Gbps stacking ports that provide an



**BROCADE**

\*Brocade HyperEdge technology is planned to be available for purchase in the first half of 2013.

## BROCADE ICX 6610 SPECIFICATIONS

### System Architecture

Connector options	<ul style="list-style-type: none"> <li>10/100/1000 ports: RJ-45</li> <li>1 Gbps SFP ports: SX, LX, LHA, LHB, 1000Base-SX, CWDM</li> <li>10 Gbps SFP+ ports: Direct-attached copper (Twinax), SR, LR</li> <li>Stacking ports: 40 QbE QSFP for use with direct-attached 1 meter or 5 meter stacking cable</li> <li>Out-of-band Ethernet management: 10/100/1000 Mbps RJ-45</li> <li>Console management: RJ-45 serial</li> </ul>
Maximum MAC addresses	32,000
Maximum VLANs	4096
Maximum STP (spanning trees)	254
Maximum routes (in hardware)	16,000
Trunking	Maximum ports per trunk: 8 Maximum trunk groups: 124
Maximum jumbo frame size	9000 bytes
Layer 2 switching	<ul style="list-style-type: none"> <li>802.1a Multiple Spanning Tree</li> <li>802.1x Authentication</li> <li>Auto MDI/MDIX</li> <li>BPDU Guard, Root Guard</li> <li>Dual-Mode VLANs</li> <li>Dynamic VLAN Assignment</li> <li>Dynamic Voice VLAN Assignment</li> <li>Fast Port Span</li> <li>GARP VLAN Registration Protocol</li> <li>IGMP Snooping (v1/v2/v3)</li> <li>Link Fault Signaling (LFS)</li> <li>MAC Address Locking; Port Security</li> <li>MAC-Layer Filtering</li> <li>MAC Learning Disable</li> <li>MLD Snooping (v1/v2)</li> <li>Multi-device Authentication</li> <li>Per-VLAN Spanning Tree (PVST/PVST+/PVRST)</li> <li>Port-based Access Control Lists</li> <li>Mirroring - Port-based, ACL-based, MAC Filter-based, and VLAN-based</li> <li>Port Loop Detection</li> <li>Private VLAN</li> <li>Protected Link Groups</li> <li>Protocol VLAN (802.1v), Subnet VLAN</li> <li>Remote Fault Notification (RFN)</li> <li>Single-instance Spanning Tree</li> <li>Single-link LACP</li> <li>Trunk Groups</li> <li>Uni-Directional Link Detection (UDLD)</li> </ul>

Base Layer 3 routing	<ul style="list-style-type: none"> <li>IPv4 and IPv6 static routes</li> <li>Host routes</li> <li>Virtual Interfaces</li> <li>Routed Interfaces</li> <li>Route-only Support</li> <li>Routing Between Directly Connected Subnets</li> </ul>
Premium Layer 3 routing	<ul style="list-style-type: none"> <li>ECMP</li> <li>L3/L4 ACLs RIP v1/v2 announce</li> <li>OSPF v2, OSPF v3 (IPv6)</li> <li>PIM-SM, PIM-SSM, PIM-DM, PIM passive (IPv4 multicast routing functionality)</li> <li>PBR</li> <li>RIP v1/v2, RIPng (IPv6)</li> <li>Virtual Route Redundancy Protocol (VRRP)</li> <li>VRRP-E, VRRP-E (IPv6)</li> <li>VRRPV3 (IPv6)</li> </ul>
Advanced Layer 3 routing	<ul style="list-style-type: none"> <li>BGP</li> </ul>
Metro features	<ul style="list-style-type: none"> <li>Metro-Ring Protocol (v1, v2)</li> <li>Virtual Switch Redundancy Protocol (VSRP)</li> <li>VLAN Stacking (Q-in-Q)</li> <li>VRRP</li> <li>Topology Groups</li> </ul>
Quality of Service (QoS)	<ul style="list-style-type: none"> <li>ACL Mapping and Marking of ToS/DSCP</li> <li>ACL Mapping and Marking of 802.1p</li> <li>ACL Mapping to Priority Queue</li> <li>ACL Mapping to ToS/DSCP</li> <li>Classifying and Limiting Flows Based on TCP Flags</li> <li>DHCP Relay</li> <li>DiffServ Support</li> <li>Honoring DSCP and 802.1p</li> <li>MAC Address Mapping to Priority Queue</li> <li>Priority Queue Management using Weighted Round Robin (WRR), Strict Priority (SP), and a combination of WRR and SP</li> </ul>

## Glosario

**AAA.**- El acrónimo AAA corresponde a un tipo de protocolos que realizan tres funciones: Autenticación, Autorización y Contabilización (Authentication, Authorization and Accounting en inglés). La expresión protocolo AAA no se refiere pues a un protocolo en particular, sino a una familia de protocolos que ofrecen los tres servicios citados.

**Algoritmo.**- Serie de pasos lógicos ordenados, que permiten resolver un problema.

**AppleTalk.**- Serie de protocolos de comunicaciones diseñados por Apple Computer. En la actualidad existen dos fases. La Fase 1, que es la versión más antigua, admite una sola red física que puede tener sólo un número de red y estar en una zona. La Fase 2, que es la versión más reciente, admite múltiples redes lógicas en una sola red física y permite que las redes se ubiquen en más de una zona.

**Arbitraje.**- Determinación de cómo negociar los accesos a un único canal de datos cuando lo están intentando utilizar varios anfitriones al mismo tiempo (evita colisiones)

**ASCII** (Código Standard Americano para el Intercambio de Información).- Este código fue propuesto por Robert W. Bemer, buscando crear códigos para caracteres alfa-numéricos (letras, símbolos, números y acentos). De esta forma sería posible que las computadoras de diferentes fabricantes logaran entender los mismos códigos.

**Broadcast.**- Mecanismo de transmisión de un nodo a múltiples nodos.

**Casas Inteligentes:** Lugares acondicionados, con diversos sistemas, equipos y redes, que facilitan las labores cotidianas, así como la estancia de las personas, dentro de estos espacios.

**CLI.**- Es un método que permite a las personas dar instrucciones a algún programa informático por medio de una línea de texto simple. Debe notarse que los conceptos de CLI, Shell y Emulador de Terminal no son lo mismo, aunque suelen utilizarse como sinónimos. Las CLI pueden emplearse interactivamente, escribiendo instrucciones en alguna especie de entrada de texto, o pueden utilizarse de una forma mucho más automatizada (batch), leyendo comandos desde un archivo de scripts.

**Código abierto.**- Código disponible para cualquier persona que quiera usarlo, modificarlo o distribuirlo

**Comunicación entre iguales.**- Proceso de interconexión de redes en el que cada capa se comunica con su capa correspondiente de la maquina destino. Las capas no se comunican directamente. Cada capa es responsable de la información de su propio encabezamiento. Las direcciones IP (lógicas) se resuelven en direcciones MAC (Físicas), de manera que puedan ser comprendidas por la siguiente capa.

**Conexión Ad Hoc.**- Es una red inalámbrica descentralizada. La red es ad hoc porque cada nodo está preparado para reenviar datos a los demás y la decisión sobre qué nodos reenvían los datos se toma de forma dinámica en función de la conectividad de la red. Esto contrasta con las redes tradicionales en las que los Routers llevan a cabo esa función. También difiere de las redes inalámbricas convencionales en las que un nodo especial, llamado punto de acceso, gestiona las comunicaciones con el resto de nodos.

**Control de flujo.**- Método que permite asegurarse de que una cantidad excesiva de datos no sobrecarga el destino. Existen 3 modalidades principales: Memoria Intermedia (buffer), Notificación de Congestión y la Técnica de ventanas.

**Correo electrónico.**- Es un servicio de red que permite a los usuarios enviar y recibir mensajes rápidamente (también denominados mensajes electrónicos o cartas electrónicas) mediante sistemas de comunicación electrónicos.

**CRC (Verificación por redundancia cíclica).**- Técnica de verificación de errores en la que el receptor de la trama calcula el resto dividiendo el contenido de la trama por un divisor binario primo y compara el resto calculado con un valor almacenado en la trama por el nodo emisor.

**dBi.**- Unidad para medir la ganancia de una antena.

**DCHP (Dynamic Host Configuration Protocol).** - Protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente. Se trata de un protocolo de tipo cliente/servidor en el que generalmente un servidor posee una lista de direcciones IP dinámicas y las va asignando a los clientes conforme éstas van estando libres, sabiendo en todo momento quién ha estado en posesión de esa IP, cuánto tiempo la ha tenido y a quién se la ha asignado después.

**DNS (Sistema de Nombres de Dominio).**- Es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes. Su función más importante, es traducir (resolver) nombres inteligibles para los humanos en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente.

**EIA/TIA-568.**- Estándar que describe las características y aplicaciones para diversos grados de tendido de cableado UTP. Ver también cableado de Categoría 1, cableado de Categoría 2, cableado de Categoría 3, cableado de Categoría 4, cableado de Categoría 5 y UTP.

**Encriptación.**- Proceso que permite transformar un mensaje, en algo inteligible que dificulta poder ser entendido.

**Estructura de trama.**- Describe la organización de los elementos de un paquete. Las máquinas en comunicación deben de utilizar tramas de la misma clase para comunicarse mutuamente el contenido real de los paquetes.

**FCS** (Secuencia de verificación de trama).- Se refiere a los caracteres adicionales que se agregan a una trama para fines de control de errores. Se usa en HDLC, Frame Relay y otros protocolos de la capa de enlace de datos.

**Fibra óptica.**- Es un medio de transmisión empleado habitualmente en redes de datos; un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. El haz de luz queda completamente confinado y se propaga por el interior de la fibra con un ángulo de reflexión por encima del ángulo límite de reflexión total, en función de la ley de Snell. La fuente de luz puede ser láser o un LED. Las fibras se utilizan ampliamente en telecomunicaciones, ya que permiten enviar gran cantidad de datos a una gran distancia, con velocidades similares a las de radio o cable.

**Firewall.**- Es una parte de un sistema o una red que está diseñada, en hardware o software, para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

**FTP** (Protocolo de Transferencia de Archivos).- Es un protocolo de red para la transferencia de archivos entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor.

**Full dúplex.**- Cualidad de los elementos que permiten la entrada y salida de datos de forma simultánea. El concepto está muy relacionado con el campo de las comunicaciones en vivo a través de la red, ya que indica que se pueden oír y hablar al mismo tiempo.

**Gateway.**- En la comunidad IP, un término antiguo que se refiere a un dispositivo de enrutamiento. En la actualidad, el término router se usa para describir nodos que ejecutan esta función, y gateway se refiere a un dispositivo con fines especiales que ejecuta conversión de capa de aplicación de la información de una pila de protocolo a otra. Comparar con router.

**GIF** (Formato de Intercambio Gráfico).- El formato fue creado por CompuServe en 1987 para dotar de un formato de imagen en color para sus áreas de descarga de ficheros, sustituyendo su temprano formato RLE en blanco y negro

**GNU.**- Proyecto de software libre creado por Richard Stallman, cuyo objetivo era el de crear, compartir y mejorar un sistema operativo tipo Unix, de código abierto.

**GPS** (Sistema Global de Navegación Satelital).- Permite establecer la posición de cualquier persona, objeto, vehículo, etc, alrededor del mundo.

**GRE** (Encapsulamiento de enrutamiento genérico). Protocolo de tunneling desarrollado por Cisco que puede encapsular una amplia variedad de tipos de paquetes de protocolo dentro de túneles IP, creando un enlace virtual punto a punto con los routers Cisco en puntos remotos a través de una internetwork IP. Al conectar subredes multiprotocolo en un entorno de backbone de un solo protocolo, el IP tunneling que usa GRE permite una ampliación de la red a través de un entorno de backbone de un solo protocolo.

**Half Dúplex**.- Método de transmisión en el que el de información es bidireccional pero no simultáneo.

**HOST**.- Sistema computacional ubicado en una red. Es similar al término nodo, salvo que el host generalmente implica un sistema computacional, mientras que el nodo generalmente se aplica a cualquier sistema conectado a la red, incluyendo servidores de acceso y routers.

**HTTP** ( Protocolo de Transferencia de Hipertexto).- HTTP define la sintaxis y la semántica que utilizan los elementos de software de la arquitectura web (clientes, servidores, proxies) para comunicarse. Es un protocolo orientado a transacciones y sigue el esquema petición-respuesta entre un cliente y un servidor. Al cliente que efectúa la petición (un navegador web o un spider) se lo conoce como "user agent" (agente del usuario). A la información transmitida se la llama recurso y se la identifica mediante un localizador uniforme de recursos (URL)

**HUB**.- Es un dispositivo que permite centralizar el cableado de una red y poder ampliarla. Esto significa que dicho dispositivo recibe una señal y repite esta señal emitiéndola por sus diferentes puertos.

**ICMP** (Internet Control Message Protocol).- Es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP). Como tal, se usa para enviar mensajes de error, indicando, por ejemplo, que un servicio determinado no está disponible o que un Router o host no puede ser localizado.

**IDF** (Intermediate Distribution Frame).- Cuarto de Telecomunicaciones secundario para un edificio que usa una topología de red en estrella. El IDF depende del MDF.

**IMAP** (Internet Message Access Protocol).- Es un protocolo de red de acceso a mensajes electrónicos almacenados en un servidor. Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet

**Interoperabilidad**.- Capacidad de los sistemas de tecnologías de la información y las comunicaciones, y de los procesos empresariales a los que apoyan, de intercambiar datos y posibilitar la puesta en común de información y conocimientos.

**Intranet.**- Red local de uso privado, que proporciona diversos servicios, muchos de los cuales están relacionados con Internet.

**Inyector PoE.**- Dispositivo que permite que los dispositivos Ethernet reciban alimentación eléctrica y datos a través del cableado de la LAN existente.

**IP (Protocolo de Internet).**- Protocolo de la capa de red de la pila TCP/IP que ofrece un servicio de internetwork sin conexión. IP proporciona características para el direccionamiento, especificación de tipo de servicio, fragmentación y reensamblaje y seguridad.

**IPX (Intercambio de paquetes de internetworking).**- Protocolo de capa de red (Capa 3) de NetWare que se usa para transferir datos desde servidores a estaciones de trabajo. El IPX es similar al IP y al XNS.

**ISP (Proveedor de Servicios de Internet).**- Agrupación o empresa dedicada al servicio de conexión, mantenimiento y prestación de servicios enfocados a Internet.

**JPEG (Grupo Conjunto de Expertos en Fotografía).**- Es el nombre de un comité de expertos que creó un estándar de compresión y codificación de archivos de imágenes fijas.

**LAN (Local Area Network).**- Es la interconexión de varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, etc.

**LAPB (Procedimiento de acceso al enlace balanceado).**- Protocolo de capa de enlace de datos de la pila de protocolo X.25. El LAPB es un protocolo orientado a bits que deriva de HDLC. Ver también HDLC y X.25.

**LAPD (Procedimiento de acceso al enlace del canal D).**- Protocolo de capa de enlace de datos RDSI para el canal D. El LAPD se deriva del protocolo LAPB y está diseñado principalmente para satisfacer los requisitos de señalización del acceso básico RDSI. Definido en las recomendaciones UIT-T Q.920 y Q.921.

**LDAP (Protocolo Ligero de Acceso a Directorios).**- Hacen referencia a un protocolo a nivel de aplicación el cual permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red.

**LLC (Control de enlace lógico).**- La más alta de las dos subcapas de la capa de enlace de datos definidas por el IEEE. La subcapa LLC administra el control de errores, el control de flujo, el entramado y el direccionamiento de la subcapa MAC. El protocolo LLC de uso

más generalizado es el IEEE 802.2, que incluye tanto variantes no orientadas a conexión como orientadas a conexión.

**MAC (Control de Acceso al Medio).**- La más baja de las dos subcapas de la capa de enlace de datos definida por el IEEE. La subcapa MAC administra acceso al medio compartido como, por ejemplo, si se debe usar transmisión de tokens o contención. Ver también capa de enlace de datos y LLC.

**MDF (Main Distribution Frame).**- Cuarto de Telecomunicaciones principal de un edificio. El Punto central de una topología de networking en estrella donde están ubicados los paneles de conexión y los dispositivos de interconexión de red principales.

**Memoria Intermedia (buffer).**- Sirven bien para ráfagas intermitentes de datos, cuando se tiene un flujo continuo excesivo de tráfico la capacidad terminara por desbordarse. Los bits se caen al suelo (ej. Fregadero).

**MTU (Unidad máxima de transmisión).**- Tamaño máximo de paquete, en bytes, que puede administrar una interfaz en particular.

**NAT (Network Address Translation).**- Mecanismo utilizado por routers y switches IP para intercambiar paquetes entre dos redes que se asignan mutuamente direcciones incompatibles. Consiste en convertir en tiempo real las direcciones utilizadas en los paquetes transportados. También es necesario editar los paquetes para permitir la operación de protocolos que incluyen información de direcciones dentro de la conversación del protocolo.

**NetBIOS (Sistema Básico de Red Entrada/Salida).**- Es un protocolo de resolución de nombres que puede ser encapsulado sobre TCP/IP. NetBIOS funciona a nivel de la capa de aplicación, dando una apariencia uniforme a todas las redes Windows independientemente de los protocolos que se hayan utilizado para las capas de red y transporte. Permite compartir archivos e impresoras así como ver los recursos disponibles en Entorno de red.

**NETWORKING.**- Conexión de cualquier conjunto de computadores, impresoras, routers, switches y otros dispositivos con el propósito de comunicarse a través de algún medio de transmisión.

**NIC (Tarjeta de Interfaz de Red).**- Dispositivo físico montado en los equipos que nos ayuda a establecer una conexión.

**Notificación de congestión.**- Se envía un mensaje a la estación de origen diciéndole que pare un momento. Cuando las memorias intermedias esta en mejores condiciones, se retransmite un nuevo mensaje indicando que puede reanudarse la transmisión. La notificación de congestión solo prolonga la agonía de que se llenen las memorias intermedias.



**Password.**- Es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso.

**PDA (Personal Digital Assistant).**- También denominado ordenador de bolsillo, es una computadora de mano originalmente diseñado como agenda electrónica (calendario, lista de contactos, block de notas y recordatorios) con un sistema de reconocimiento de escritura.

**Pila.**- Estructura de datos donde el último dato que entra es el primero que sale.

**Ping.**- Utilidad diagnóstica en redes de computadoras que comprueba el estado de la conexión del host local con uno o varios equipos remotos por medio del envío de paquetes ICMP de solicitud y de respuesta. Mediante esta utilidad puede diagnosticarse el estado, velocidad y calidad de una red determinada

**Fishing.**- Adquisición de información de manera ilegal.

**POP3 (Protocolo de oficina de correos).**- Como su nombre lo indica, permite recoger el correo electrónico en un servidor remoto (servidor POP)

**Portal Cautivo (o Captivo).**- Es un programa o máquina de una red informática que vigila el tráfico HTTP y fuerza a los usuarios a pasar a los usuarios a pasar por una página especial si quieren navegar por Internet de forma normal.

**Protocolo.**- Conjunto de reglas y procedimientos, establecidos para realizar una acción.

**Punto de acceso.**- Dispositivo que interconecta dispositivos de comunicación inalámbrica para formar una red inalámbrica.

**QoS.**- Referencia a la Calidad del Servicio.

**RADIUS (Remote Authentication Dial-In User Server).**- Es un protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP. Utiliza el puerto 1813 UDP para establecer sus conexiones.

**Recurso.**- Cualquier componente que es utilizado, o interviene directa o indirectamente dentro de cualquier actividad, esquema, sistema, etc.

**Red de computadoras.**- Es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos. Este término también engloba aquellos medios técnicos que permiten compartir la información.

**Red.**- Conjunto de dispositivos conectados por un medio, a través del cual se pueden compartir y utilizar archivos, recursos y servicios.

**RedUNAM.**- Sistema autónomo de la UNAM que está compuesto por un conjunto de redes locales que tienen una administración propia, pero al estar conectadas a toda la red sus encargados y usuarios deben acatar las disposiciones establecidas por la Dirección de Telecomunicaciones.

**RIP** (Protocolo de información de enrutamiento).- IGP que se suministra con los sistemas UNIX BSD. El IGP más común de Internet. El RIP usa el número de saltos como métrica de enrutamiento.

**Router.**- Dispositivo de capa de red que usa una o más métricas para determinar la ruta óptima a través de la cual se debe enviar el tráfico de red. Los routers envían paquetes desde una red a otra basándose en la información de la capa de red. Ocasionalmente se denomina gateway (aunque esta definición de gateway se está tornando cada vez más desactualizada). Comparar con gateway.

**RPC** (Llamada a Procedimiento Remoto).- Protocolo que permite a un programa de ordenador ejecutar código en otra máquina remota sin tener que preocuparse por las comunicaciones entre ambos.

**RS-232.**- Interfaz de capa física popular. En la actualidad se denomina EIA/TIA-232. Ver EIA/TIA-232.

**Smartphone.**- Es un término comercial para denominar a un teléfono móvil que ofrece más funciones que un teléfono celular común. Casi todos los teléfonos inteligentes son móviles que soportan completamente un cliente de correo electrónico con la funcionalidad completa de un organizador personal. Una característica importante de casi todos los teléfonos inteligentes es que permiten la instalación de programas para incrementar el procesamiento de datos y la conectividad. Estas aplicaciones pueden ser desarrolladas por el fabricante del dispositivo, por el operador o por un tercero. El término "Inteligente" hace referencia a cualquier interfaz, como un teclado QWERTY en miniatura, una pantalla táctil, o simplemente el sistema operativo móvil que posee, diferenciando su uso mediante una exclusiva disposición de los menús, teclas, atajos, etc.

**SMTP** (Protocolo de transporte de correo simple).- Es un protocolo de la capa de aplicación. Protocolo de red basado en textos utilizados para el intercambio de mensajes de correo electrónico entre computadoras u otros dispositivos (PDA's, teléfonos móviles, etc.)

**SNMP** (Protocolo simple de administración de red).- Protocolo de la capa de aplicación que facilita el intercambio de información de administración entre dispositivos de red. Es parte de la familia de protocolos TCP/IP. SNMP permite a los administradores supervisar el funcionamiento de la red, buscar y resolver sus problemas, y planear su crecimiento. Las versiones de SNMP más utilizadas son SNMP versión 1 (SNMPv1) y SNMP versión 2 (SNMPv2).

**SPX** (Intercambio de paquete secuenciado).- Protocolo confiable, orientado a conexión que complementa el servicio de datagrama suministrado por los protocolos de capa de red (Capa 3). Novell derivó este protocolo de transporte NetWare de uso generalizado del SPP del conjunto de protocolos XNS.

**SQL** (Lenguaje de Consulta Estructurado).- Es un lenguaje declarativo de acceso a bases de datos relacionales que permite especificar diversos tipos de operaciones en estas.

**SSH** (Secure SHell).- Nombre de un protocolo y del programa que lo implementa, y sirve para acceder a máquinas remotas a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

**SSID** (Service Set IDentifier).- Es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red.

**Subneteo**.- Proceso mediante el cual se puede dividir un segmento de direcciones IP en varios subsegmentos.

**Subred**.- Grupo de direcciones IP que tienen el mismo valor en la primera parte de las direcciones IP, con el fin de que el enrutamiento pueda identificar el grupo por esa parte inicial de las direcciones. Las direcciones IP de la misma subred normalmente se asientan en el mismo medio de red y no están separados entre sí por routers. Las direcciones IP de subredes diferentes están separadas entre sí normalmente por al menos un router.

**Switch**.- Dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

**TCP** (Protocolo de control de transmisión).- Protocolo de capa de transporte orientado a conexión que suministra transmisión de datos full-duplex confiable. El TCP forma parte de la pila de protocolo TCP/IP. Ver también TCP/IP.

**Técnica de ventanas**.- Se permite la transferencia de un número acordado de paquetes, antes de que se precise un acuse de recibo por parte del receptor. (no podrá sobrecargarse fácilmente). Debe esperar a que la estación remota responda antes de enviarle más datos.

**Tecnología**.- Conjunto de conocimientos aplicables, orientados a resolver necesidades de un modo práctico.

**Telnet** (TELEcommunication NETwork).- Protocolo de red que sirve para acceder mediante una red a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella. El puerto que se utiliza generalmente es el 23.

**TFTP** (Trivial File Transfer Protocol).- Es un protocolo de transferencia muy simple semejante a una versión básica de FTP. TFTP a menudo se utiliza para transferir pequeños archivos entre ordenadores en una red, como cuando un terminal X Window o cualquier otro cliente ligero arranca desde un servidor de red.

**Transceiver**.- Dispositivo que tiene un transmisor y un receptor que se combinan y los circuitos de acciones ordinarias o de una sola cubierta. Si no es común entre los circuitos de transmisión y recepción de las funciones, el dispositivo es un transmisor-receptor.

**Trunk**.- En el contexto de las VLANs, el término trunk ('troncal') designa una conexión de red que transporta múltiples VLANs identificadas por etiquetas (o tags) insertadas en sus paquetes.

**UDP** (Protocolo de Datagrama de Usuario).- Protocolo de la capa de transporte no orientado a conexión de la pila de protocolos TCP/IP. El UDP es un protocolo simple que intercambia datagramas sin acuses de recibo ni garantía de envío, que requiere que el procesamiento de errores y la retransmisión sean administrados por otros protocolos. El UDP se define en la RFC 768.

**URL** (Localizador Uniforme de Recursos).- Cadena de caracteres que asigna una dirección única a cada uno de los recursos disponibles dentro de Internet.

**VLAN**.- Es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un único switch o en una única red física. Son útiles para reducir el tamaño del dominio de broadcast y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador o un switch capa 3 y 4).

**WEP** (Wired Equivalent Privacy).- Sistema de cifrado incluido en el estándar IEEE 802.11 como protocolo para redes Wireless que permite cifrar la información que se transmite. Proporciona un cifrado a nivel 2, basado en el algoritmo de cifrado RC4 que utiliza claves de 64 bits (40 bits más 24 bits del vector de iniciación IV) o de 128 bits (104 bits más 24 bits del IV).

**Wifi Hopper**.- Programa informático que permite al usuario explorar un área geográfica determinada para detectar redes inalámbricas. Puede enlistar los detalles de la red incluyendo SSID, MAC address, señal, modo de la red, el estado del cifrado (WEP, WPA), la frecuencia y el canal.

**Wireshark.**- Antes conocido como Ethereal, es un analizador de protocolos utilizado para realizar análisis y solucionar problemas en redes de comunicaciones para desarrollo de software y protocolos, y como una herramienta didáctica para educación. Cuenta con todas las características estándar de un analizador de protocolos.

**WPA (Wi-Fi Protected Access).**- Es un sistema para proteger las redes inalámbricas; creado para corregir las deficiencias del sistema previo WEP.

**10BASE-T,** es una variedad del protocolo de red Ethernet recogido en la revisión IEEE 802.3i en 1990 que define la conexión mediante cable de par trenzado. Utilizada para cortas distancias debido a su bajo costo

**802.11.-** El estándar IEEE 802.11 define el uso de los dos niveles inferiores de la arquitectura OSI (capas física y de enlace de datos), especificando sus normas de funcionamiento en una WLAN.

## **Bibliografía.**

Integrating IPv6 into Your IPv4 Network  
IPv6 Essentials  
O'Reilly, Silvia Hagen.

IPv6 Network Programming .  
Jun-ichiro-itojun Hagino  
Elsevier. Digital Press

Voice Over IPv6  
Daniel Minoli  
Elsevier

Deploying IPv6 Networks  
Axel Clauberg  
Cisco

Dye, Mark A. McDonald, Rick. W. Rufi, Antoon.  
“Aspectos básicos de networking.”  
CISCO NETWORK ACADEMY, 2008.

Cisco System Learning.  
“Interconnecting Cisco Networking Devices.”  
Volumen 1, versión 1.0.  
Student Guide, 2010.

Cisco System Learning.  
“Interconnecting Cisco Networking Devices.”  
Volumen 2, versión 1.0.  
Student Guide, 2010.

ARUBA NETWORKS.  
“Implementing Aruba WLAN’s”  
Student Guide, 2009.

ARUBA NETWORKS.  
“Scalable WLAN desing & Implementation.”  
Student Guide, 2009.

Norma oficial Mexicana NOM-121-SCT1-2009  
Diario Oficial, Lunes 21 de junio de 2010

### **Páginas web consultadas.**

<http://www.apple.com/mx/macosex/server/features/all.html>  
<http://es.wikipedia.org/wiki/IPv6>  
<http://es.wikipedia.org>  
[www.eluniversal.com.mx](http://www.eluniversal.com.mx)