

INSTITUTO TECNOLÓGICO Y DE ESTUDIOS SUPERIORES DE OCCIDENTE

MAESTRÍA EN INFORMÁTICA APLICADA

Reconocimiento de Validez Oficial de Estudios de Nivel Superior según acuerdo secretarial
15018, publicado en el
Diario Oficial de la Federación el 29 de noviembre de 1976.



Implementación de IPv6 para la certificación de plataformas móviles INTEL para Android: un estudio de caso

Tesis que para obtener el título de

Maestro en Informática Aplicada

Presenta:

Juan Carlos López Dávila

Asesor:

Mtro. Álvaro Iván Parres Peredo

Guadalajara, Jalisco

Diciembre de 2015

CONTENIDO	5
ÍNDICE DE TABLAS	5
ÍNDICE DE ILUSTRACIONES	6
I. INTRODUCCION	8
I.1 CONSIDERACIONES DE CONFIDENCIALIDAD.	8
I.2 ANTECEDENTES	8
I.3 JUSTIFICACIÓN	11
I.4 OBJETIVO.....	12
II. MARCO TEÓRICO	12
II.1 REDES DE COMPUTADORAS	12
II.1.1 Modelo OSI.....	13
II.1.2 Capa de Red.....	16
II.1.3 IP.....	18
II.1.4 IPv4	19
II.1.5 Motivaciones para IPv6.....	25
II.1.6 IPv6	25
Transición de IPv4 a IPv6	28
II.1.7.....	28
II.1.8 Mecanismos de Transición	29
II.2 DISPOSITIVOS MÓVILES	31
II.3 DISPOSITIVOS MÓVILES EN LA ACTUALIDAD.	31
II.4 SISTEMAS OPERATIVOS MOVILES	33
II.5 GOOGLE	36
II.5.1 Google INC.....	36

II.5.2	<i>Android</i>	37
II.5.3	<i>Android Compatible</i>	39
II.5.4	<i>Compatibility Test Suite</i>	41
II.6	INTEL	42
II.6.1	<i>INTEL Corporation</i>	42
II.6.2	<i>Procesadores INTEL en plataformas Móviles.</i>	43
II.7	METODOLOGÍA DE IMPLEMENTACIÓN DE DUAL STACK NIST	44
III.	MARCO METODOLÓGICO	46
III.1	DE LA INVESTIGACIÓN	46
III.2	DE LA ADECUACIÓN DEL LABORATORIO DE INTEL EN RUMANIA PARA EL SOPORTE DE IPV6	
	47	
IV.	DESARROLLO	48
IV.1	INICIO DEL PROYECTO.....	48
IV.2	FASE DE ANÁLISIS	49
IV.2.1	<i>Recabar Requerimientos</i>	50
IV.2.2	<i>Expectativas del cliente</i>	50
IV.2.3	<i>Topología IPv4 del laboratorio</i>	50
IV.2.4	<i>Restricciones del Laboratorio</i>	53
IV.3	FASE DE DISEÑO	54
IV.3.1	<i>Firewall Transparente</i>	54
IV.3.2	<i>IPv6 subred única con DHCPv6 en el firewall</i>	56
IV.3.3	<i>IPv6 subred única con SLAAC en el firewall</i>	57
IV.3.4	<i>Múltiples Redes Ipv6 Con Dhcpv6 En El Access Point</i>	62
IV.3.5	<i>Presentación De La Propuesta De Implementación Al Cliente</i>	66
	FASE DE IMPLEMENTACIÓN.....	66

IV.4	66
IV.4.1	<i>Documentación Del Cambio</i>66
IV.4.2	<i>Ventana De Mantenimiento</i>67
IV.4.3	<i>Implementación Del Cambio</i>68
V.	RESULTADOS68
V.1	VERIFICACIÓN INTERNA.....69
V.2	VERIFICACIÓN EXTERNA.....72
V.3	VALIDACIÓN DEL USUARIO FINAL.....74
VI.	CONCLUSIONES74
VII.	PROPUESTA DE MEJORA76
VIII.	BIBLIOGRAFÍA79
IX.	ANEXOS81
IX.1	ANEXO 1. COMUNICACIÓN DE LA FINALIZACIÓN DE LA IMPLEMENTACIÓN81
IX.2	ANEXO 2. CONFIRMACIÓN DEL LÍDER DE PROYECTO SOBRE LA FUNCIONALIDAD DEL LABORATORIO82
IX.3	ANEXO 3. BUSCANDO LA AUTORIZACIÓN PARA LA IMPLEMENTACIÓN DEL CAMBIO82
IX.4	ANEXO 4. AUTORIZACIÓN DEL CLIENTE83
IX.5	ANEXO 5. VENTANA AGENDADA.....83

CONTENIDO

Índice de Tablas

Tabla 1. Bloques reservados para direcciones privadas	25
Tabla 2. Distribución del mercado mundial de Sistemas Operativos móviles (IDC Research, Inc 2015)	32
Tabla 3. Cuota del mercado global de smartphones en el segundo cuarto de 2015 (IDC Research, Inc 2015)	33
Tabla 4. Comparativa entre Sistemas Operativos para Móviles (Rivera y Van der Meulen 2015)	33

Índice de Ilustraciones

Ilustración 1. Capas del modelo de referencia OSI (Kurose & Ross, 2012)	14
Ilustración 2. Ejemplo de una tabla de ruteo	17
Ilustración 3. Funciones y características de la Capa de Red. (Kurose & Ross 2012). 17	
Ilustración 5. Paquete IP dentro de una trama de la Capa de Enlace	18
Ilustración 6. Dirección IPv4 en binario y en notación decimal con puntos	23
Ilustración 7. Direcciones IP asignadas a interfaces de hosts y de un ruteador (Kurose & Ross 2012)	24
Ilustración 8. Estructura de un datagrama IPv4 (Kurose & Ross 2012)	21
Ilustración 9. Estructura de un datagrama IPv6. (Kurose & Ross 2012)	27
Ilustración 10. Concepto de Dual Stack (Afifi y Toutain 1999)	30
Ilustración 11. Interfaz gráfica de IOS versión 9 (Apple, 2015)	35
Ilustración 12. Página principal de Windows Phone 8 (Winsupersite, 2015)	36
Ilustración 13. Arquitectura de Android (Gandhewar y Sheikh 2010)	39
Ilustración 14. Diagrama de red del laboratorio de INTEL Rumania	51
Ilustración 15. Distribución de redes dentro del laboratorio	52
Ilustración 16. Topología de red con un firewall transparente	55
Ilustración 17. Firewall haciendo la función de servidor DHCPv6	56
Ilustración 18. Router anunciando el prefijo de la red a través de los RA	58
Ilustración 19. Topología física del laboratorio	61
Ilustración 20. Topología lógica del laboratorio	61
Ilustración 21. Configuración de IPv6 en el equipo DIR-600	63

Ilustración 22. Access Point como servidor DHCPv6 y Gateway de la red	64
Ilustración 23. Nueva topología del laboratorio	65
Ilustración 24. Configuración IPv6 del Ruteador Inalámbrico.....	69
Ilustración 25. Configuración IPv6 del Ruteador Inalámbrico.....	70
Ilustración 26. Página de Administración IPv6 del Ruteador Inalámbrico	70
Ilustración 27. Interfaces del firewall con IPv4 e IPv6	71
Ilustración 28. Tabla de ruteo IPv6 del firewall.....	71
Ilustración 29. Reglas de acceso IPv6 del firewall	71
Ilustración 30. Conectividad IPv6 exitosa entre el laboratorio y el ISP.....	72
Ilustración 31. Ping desde la red interna hacia Internet	72
Ilustración 32. Traza IPv6 desde el laboratorio hacia Internet.....	72
Ilustración 33. Página IPv6 de Facebook	73
Ilustración 34. Cliente sin soporte para IPv6	73
Ilustración 35. Laboratorio de Rumania IPv6 funcionando	74

I. INTRODUCCION

I.1 Consideraciones de Confidencialidad.

El presente trabajo omite diversos nombres, correos, direcciones y otra información sensible por cuestiones de confidencialidad de la empresa donde se realizó el proyecto. A lo largo del documento se podrán encontrar secciones ocultas o nombres modificados para respetar lo anterior.

I.2 Antecedentes

INTEL es una compañía dedicada al diseño y manufactura de microprocesadores, así como los componentes necesarios para su correcto funcionamiento. La compañía como parte de su proceso evolutivo ha incrementado su portafolio de productos que incluyen el diseño y manufactura de microprocesadores y tarjetas madre para servidores, laptops y computadoras personales; incluyendo el diseño y la fabricación de componentes de hardware como tarjetas de video, de red y procesadores para dispositivos móviles por mencionar algunos.

Compañías como INTEL, AMD y ARM desarrollan procesadores y tarjetas madre que procesan los datos generados por los usuarios. Estas organizaciones proporcionan parte de la infraestructura necesaria para el procesamiento y transmisión de información. La cual es utilizada por proveedores de servicio y usuarios ávidos de consultar y generar contenidos.

Un ingrediente tecnológico que ha acelerado esta necesidad de acceso a la información son los dispositivos móviles. Estos dispositivos electrónicos proporcionan a los usuarios capacidades similares a las laptops o computadoras de escritorio, pero con un poder de

procesamiento menor. Ahora es posible hacer reservaciones a hoteles desde un teléfono o acceder a las redes sociales desde una tableta por citar algunos ejemplos. De acuerdo a Church (2007) estos dispositivos se están convirtiendo en la principal plataforma de acceso a la información predilecta para los usuarios, comenzado a superar a las computadoras personales.

El teléfono móvil es la tecnología que ha sido adoptada con mayor rapidez en la historia del mundo, los países más industrializados, miembros de la OCDE, tienen en promedio un 70% de la población que los utiliza (Arminen 2007). Estos dispositivos están en constante evolución; han reducido su tamaño, tienen una mayor duración de la batería, mejores métodos de señalización y cada vez tienen más funcionalidades. En décadas anteriores tener música, llamadas telefónicas y reloj requería de tres aparatos distintos; mientras que hoy se puede tener lo anterior y más en un solo dispositivo.

Una de las estrategias de INTEL para incrementar sus ventas, es la de impulsar diversas tecnologías que aprovechen las capacidades del hardware que esta compañía diseña y manufactura. La mayoría de las tecnologías que INTEL impulsa se relacionan con tecnologías *Open Source*¹ de las cuales es un gran contribuidor. Recientemente INTEL ha estado desarrollando procesadores y hardware para plataformas móviles como lo son los teléfonos inteligentes y tabletas. La arquitectura INTEL para móviles está diseñada para correr el sistema operativo Android² de Google.

1 Open Source se refiere a cualquier programa informático que puede ser modificado por cualquier usuario y que su código fuente está abierto

2 Android es un Sistema Operativo basado en Linux desarrollado por Google enfocado a teléfonos inteligentes y Tablets

El sistema operativo Android está diseñado para correr sobre diferentes arquitecturas de procesadores; pero las aplicaciones, su desarrollo y funcionalidad deben ser las mismas para cualquier teléfono o tableta. En el sitio de Android (2015) se puede leer: “*El propósito de Android es del establecer una plataforma abierta para desarrolladores para crear aplicaciones novedosas*”.

Esta versatilidad y evolución de los dispositivos móviles se ha logrado gracias a que grandes compañías, tanto de software como de hardware, han incursionado en el mercado de dispositivos móviles. Según Smith (2008) INTEL y ARM están librando una dura batalla en el campo de los procesadores móviles; mientras que Microsoft, Google y Apple luchan por tener supremacía en los sistemas operativos para estos dispositivos. Tanto para INTEL como para estas compañías este segmento se ha vuelto de vital importancia.

Para que un dispositivo sea certificado por Google como compatible con Android se necesitan realizar tres pasos:

1. Obtener el código fuente de Android para la plataforma deseada ya sea INTEL ARM o alguna otra.
2. Cumplir con el Documento de Definición de Compatibilidad para (*Android Compatibility Definition Document*)
3. Aprobar la Suite de Pruebas de Compatibilidad (CTS por sus siglas en inglés).

El programa de compatibilidad con Android busca hacer más sencillo para los fabricantes de dispositivos móviles el desarrollar dispositivos compatibles con Android.

Con un 5% del total del mercado global en *tablets* y menos de un 1% en *smartphones* INTEL se encuentra rezagado en relación con sus competidores (Trefis.com 2015). Empresas como ARM o Motorola son las que tienen el dominio del mercado de procesadores para este tipo de dispositivos.

Ante la pérdida de participación de mercado en los segmentos donde típicamente INTEL es líder y con la meta de introducir 70 millones de *tablets* al mercado en 2015 INTEL no puede darse el lujo de tener errores o retrasos en el lanzamiento de sus productos para este segmento (AndroidHeadlines.com 2014). Pasar exitosamente pruebas como el CTS de Google es clave para evitar retrasos. Este tipo de pruebas requieren una infraestructura tecnológica que permita que estas puedan ser ejecutadas con éxito.

La necesidad de probar una plataforma y la urgencia para que esta pudiera salir al mercado en tiempo y forma obligo a adecuar la infraestructura existente en un laboratorio para poder llevar acabo las pruebas exigidas por Google. Y es precisamente este tópico la motivación de este trabajo, el cual se realiza en el contexto de INTEL.

I.3 Justificación

El presente proyecto, de adecuar la infraestructura de un laboratorio de INTEL en Rumania para soportar IPv6, surge a raíz de la necesidad de poder certificar en tiempo y forma los dispositivos móviles sobre plataforma Android y evitar de esta forma las perdidas económicas que esto pudiera provocar.

I.4 Objetivo

Adecuar un laboratorio dentro de las instalaciones de INTEL Rumania con el fin de poder realizar en este la totalidad de las pruebas requeridas por Google con el fin de certificar que los dispositivos móviles con plataforma INTEL son compatibles con el sistema operativo Android.

II. MARCO TEÓRICO

II.1 Redes de Computadoras

El término redes de computadoras ha sido definido por diversos autores. Algunas de estas definiciones son:

Para Tenenbaum (2003) una red de computadoras es “Un conjunto de computadoras autónomas que pueden intercambiar información sin importar el medio físico por el cual se realice ese intercambio”. El mismo Tanenbaum resalta que la diferencia entre una red de computadoras y un sistema distribuido es que este último es un conjunto de computadoras independientes que aparecen al usuario como un sistema único.

Odom (2008) por su parte define a las redes de computadoras como: “Una colección de computadoras, impresoras, ruteadores, switches y otros dispositivos que se pueden comunicar entre ellos sobre algún medio de transmisión”.

Mientras que Olifery Olifer (2009) aseguran lo siguiente: “Las redes de computadoras, también conocidas como redes de comunicación de datos o de transmisión de datos, representan el resultado lógico de la evolución de dos de las ramas científicas y

tecnológicas más importantes de la civilización moderna: las tecnologías de computadoras y de las telecomunicaciones”.

II.1.1 Modelo OSI

Con el fin de crear una arquitectura en la transmisión de datos a través de una red la ISO3 en 1984 desarrolla el estándar *Open Systems Interconnection* (OSI). Según Zimmermann (1990): “El objetivo de la SC16⁴ es el de estandarizar las reglas de interacción entre sistemas interconectados. Por lo tanto, el comportamiento externo de los sistemas abiertos deberá alienarse conforme a la arquitectura de la OSI mientras que la organización interna y el funcionamiento de dichos sistemas esta fuera del campo de acción de los estándares de la OSI.”

El modelo OSI representa la lógica para enviar datos. Es importante recordar que este modelo no especifica cómo se debe realizar el envío y recepción de los datos, solamente define que es necesario. Distintos protocolos pueden implementar funciones de manera diferente. Por ejemplo, el estándar abierto de IP (*Internet Protocol*) y el de IPX (*Internetwork Packet Exchange*) de Novell son implementaciones distintas de la capa de red. Teare (2008).

Kurose and Ross (2012) afirman que, para proveer estructura de diseño a los protocolos de red, los diseñadores de red organizaron dichos protocolos por capas. Cada protocolo pertenece a una capa. Cada una de estas capas provee su servicio de dos formas:

1. Al realizar funciones dentro de esa capa

3 International Organization for Standardization. Organización independiente y no gubernamental que desarrolla estándares para diferentes tecnologías y procesos

4 Comité creado por la ISO para desarrollar el estándar OSI

2. Utilizando los servicios de la capa inferior

La Ilustración 1 muestra las capas que conforman el modelo OSI

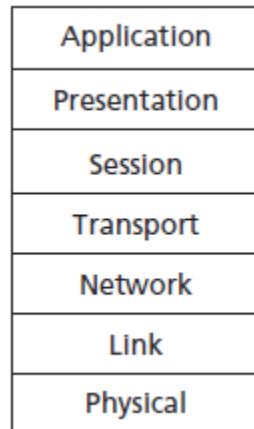


Ilustración 1. Capas del modelo de referencia OSI (Kurose & Ross, 2012)

A continuación, se detalla cada una de las capas del Modelo OSI:

- **Capa de Aplicación.** En esa capa es donde las aplicaciones de red y los protocolos de la capa de aplicación residen. Algunos de estos protocolos son: HTTP⁵, FTP⁶, DNS ⁷y SMTP⁸. Un protocolo de la capa de aplicación está distribuido entre múltiples sistemas; en clientes con aplicaciones que utilizan el protocolo para intercambiar paquetes de información con servidores los cuales tienen aplicaciones para procesar las peticiones de los clientes. Los paquetes de información en la capa de información se conocen como mensajes. (Kurose and Ross 2012)

5 Protocolo de Hipertransferencia de Texto. Protocolo utilizado para la visualización de páginas web.

6 Protocolo de Transferencia de archivos. Protocolo utilizado para transferir archivos entre servidores

7 Servidor de Nombres de Dominio. Protocolo utilizado para convertir nombres en IPs

8 Protocolo Simple de Transferencia de Correo. Protocolo utilizado para el envío y recepción de correos.

- **Capa de Presentación.** El propósito principal de la Capa de Presentación es el de proveer independencia a los procesos de las aplicaciones de las diferencias en la representación de datos, por ejemplo, la sintaxis. La Capa de Presentación puede ser específica a una aplicación en particular. (Zimmermann 1990)
- **Capa de Sesión.** “El propósito de la Capa de Sesión es el de proveer mecanismos para organizar y estructurar la interacción entre los procesos de las aplicaciones. En esencia esta capa provee la estructura para controlar la comunicación”. (Zimmermann 1990)
- **Capa de Transporte.** La Capa de Transporte transporta mensajes de la capa de aplicación entre dos dispositivos. En Internet hay dos protocolos de transporte: UDP ⁹y TCP¹⁰. Mientras TCP asegura la entrega de los paquetes y tiene mecanismos de retransmisión UDP carece de ellos. Los paquetes de la capa de transporte son mejor conocidos como segmentos (Kurose and Ross 2012).
- **Capa de Red.** La capa de red es la responsable de mover paquetes de red entre hosts. Estos paquetes se conocen como datagramas. Esta capa provee el servicio de entregar los segmentos de la capa de transporte hacia el host destino (Kurose and Ross 2012).
- **Capa de Enlace.** La finalidad de la Capa de Enlace es proveer la funcionalidad y los procedimientos para transferir datos entre entidades de red, así como detectar y posiblemente corregir errores que puedan ocurrir en la Capa Física. Protocolos típicos de esta capa son: HDCL para enlaces punto a punto y multipunto y el IEEE

9 User Datagram Protocol. Protocolo utilizado para la transmisión de datos. Este protocolo no es orientado a la conexión.

10 Transport Control Protocol. Protocolo utilizado para la transmisión de datos. Es un protocolo orientado a la conexión.

802 para redes locales. Los protocolos de esta capa son muy sensibles a la tecnología de transferencia. Mientras que en capas superiores existe un protocolo por capa, en las capas inferiores este no es el caso. (Zimmermann 1990)

- **Capa Física.** El trabajo de la Capa física es el de mover bits individuales de un nodo al siguiente. Los protocolos de esta capa dependen del medio sobre el cual van a trabajar. Por ejemplo, Ethernet tiene varios protocolos de capa física: uno para cable cruzado de cobre, otro para fibra óptica y otro para cable coaxial, por mencionar algunos. Dependiendo el medio físico los bits se transferirán de forma distinta. (Kurose and Ross 2012)

II.1.2 Capa de Red

La Capa de Red del modelo OSI es la encargada de las comunicaciones de extremo a extremo entre dispositivos ubicados en diferentes redes. Esta capa tiene tres principales características: direccionamiento lógico, ruteo y reenvío de paquetes (Odom 2008).

Kurose & Rose (2012) explican las funciones de ruteo y determinación de rutas de la siguiente manera:

- **Reenvío de Paquetes.** El proceso por el cual un ruteador recibe un paquete por una de sus interfaces y determina por cuál de sus interfaces debe ser reenviado dicho paquete. Para lograr lo anterior, los ruteadores se basan en su tabla de ruteo. Esta tabla contiene una lista de redes y a través de que interface o siguiente salto se pueden alcanzar. La Ilustración 2 muestra un ejemplo de una tabla de ruteo.


```
ST-SW-501.1 # show iproute
```

Ori	Destination	Gateway	Mtr	Flags
#s	Default Route	192.168.0.129	1	UG---S-um--f-
#s	172.22.200.0/23	192.168.0.129	1	UG---S-um--f-
#d	192.168.0.128/25	192.168.0.131	1	U-----um--f-
#d	192.168.30.0/24	192.168.30.2	1	U-----um--f-
#d	192.168.100.0/25	192.168.100.2	1	U-----um--f-
#d	192.168.104.0/23	192.168.104.2	1	U-----um--f-
#d	192.168.106.0/23	192.168.106.2	1	U-----um--f-
#d	192.168.108.0/23	192.168.108.2	1	U-----um--f-
#d	192.168.110.0/23	192.168.110.2	1	U-----um--f-
#d	192.168.112.0/23	192.168.112.2	1	U-----um--f-

Ilustración 2. Ejemplo de una tabla de ruteo

- **Ruteo.** La capa de red debe determinar la ruta o camino que los paquetes deben tomar mientras son transmitidos del emisor al receptor. Los algoritmos que calculan estas rutas se conocen como algoritmos de ruteo. Algunos algoritmos de ruteo son EIGRP¹¹, OSPF ¹²y BGP ¹³por mencionar algunos.

La Ilustración 3 hace un resumen grafico de las funciones y componentes de la capa de red.

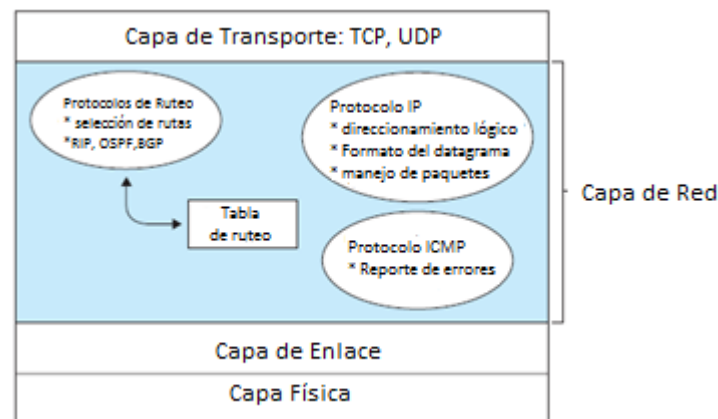


Ilustración 3. Funciones y características de la Capa de Red. (Kurose y Ross 2012)

11 Enhanced Interior Gateway Protocol. Protocolo de ruteo propietario de Cisco.

12 Open Shortest Path First. Potocolo de ruteo abierto. Utiliza el algoritmo de Djisktra para buscar la mejor ruta.

13 Border Gateway Protocolo. Protocolo de ruteo utilizado para rutear en Internet.

El direccionamiento en esta capa se realiza utilizando el protocolo IP¹⁴. Actualmente existen dos versiones, las cuales se explicaran a continuación.

II.1.3 IP

El Protocolo de Internet (IP por sus siglas en inglés) es el protocolo primario de la capa de red del modelo OSI y provee funciones de interconexión entre redes. Su función primaria es la de proveer direccionamiento lógico y rutear paquetes entre hosts. IP ha perdurado desde que fue formalizado en el RFC 791 en 1981 (Davies 2008).

La Ilustración 4 muestra un datagrama IP encapsulado en una trama de la capa de enlace.

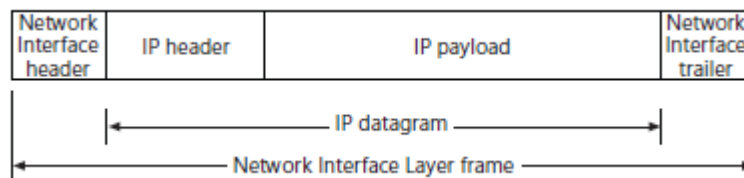


Ilustración 4. Paquete IP dentro de una trama de la Capa de Enlace

(Davies 2008)

El propósito principal de IP es el de mover datagramas entre redes interconectadas. Esto se logra pasando datagramas desde un módulo de internet hacia otro sucesivamente hasta que se alcance el destino. Los módulos de internet residen en los hosts y las puertas de enlace en el sistema de internet. Dichos datagramas son ruteados de un módulo a otro a través de redes individuales basado en la interpretación de las

¹⁴ Internet Protocol.

direcciones de internet. Por lo tanto, un mecanismo importante de IP son las direcciones (RFC 791 1981).

Olifer y Olifer (2009) afirman lo siguiente: “IP es un protocolo sin conexión, lo que significa que procesa cada paquete IP como una unidad independiente. Además, IP no tiene mecanismos para asegurar la autenticidad de los paquetes ni para la corrección de errores durante la transmisión. Si se ha presentado algún error durante el envío del paquete, IP no inicia ninguna acción para corregirla”.

IP sin importar que versión sea, utiliza direcciones lógicas para transmitir datos entre nodos en una red. El RFC 791 (1981) establece que: “El protocolo de Internet ofrece para la transmisión de bloques de datos llamados datagramas de fuentes a los destinos, donde las fuentes y los destinos son hosts identificados por direcciones de longitud fija. El protocolo de Internet también proporciona mecanismos para la fragmentación y reensamblaje de datagramas largos, si es necesario”.

En la actualidad existen dos versiones del protocolo IP: IPV4 e IPV6.

II.1.4 IPv4

IPv4 es la primera versión del protocolo IP, este protocolo está especificado en el RFC 791 (1981). Actualmente IPv4 es la versión de IP mayormente utilizada en las redes del mundo.

II.1.4.1 *Formato de los Datagramas IPv4*

El formato de un datagrama de IPv4 consta de 14 campos, los cuales según el RFC 791 (1981) son:

- **Versión.** Campo de 4 bits que especifica la versión del Protocolo IP.
- **Longitud del Encabezado.** Indica la longitud del encabezado en palabras de 32 bits. Su valor mínimo es 5 mientras que el máximo es 15. Este campo típicamente es de 20 bytes.
- **Tipo de Servicio.** El propósito de este campo es el de distinguir entre las diferentes clases de servicios. Es un campo que los ruteadores ignoran a menos que se indique lo contrario. La longitud de este campo es de 6 bits.
- **Longitud Total.** El tamaño total del paquete (incluyendo el encabezado) medido en bytes. Este campo es de 16 bits.
- **Identificación.** Campo utilizado para que un host pueda determinar a qué datagrama corresponde un fragmento recién llegado.
- **Banderas.** Consta de tres campos de 1 bit. El primer campo no se utiliza. El segundo campo es el DF (don't fragment), es una orden para los ruteadores para no fragmentar un datagrama. El tercer campo es MF (more fragments) es necesario para determinar si se recibieron todos los fragmentos de un datagrama.
- **Desplazamiento del Fragmento.** Este campo indica en que parte del datagrama actual va el fragmento. Este campo es de 13 bits.
- **Tiempo de Vida.** Es un contador que sirve para limitar la vida de un paquete. Este campo disminuye cada vez que es procesado por un ruteador. Cuando el tiempo de vida es 0, el datagrama se descarta.
- **Protocolo.** Este campo indica el protocolo de las capas superiores al que el datagrama debe entregarse. Para TCP el valor es 6, mientras que para UDP es 17.

- **Suma de Verificación del Encabezado.** Verifica solamente el encabezado. Es un mecanismo útil para la detección de errores. Este campo se recalcula cada que un paquete es procesado por un ruteador. Si un ruteador detecta un error en un paquete, este es descartado.
- **Dirección Origen y Destino.** Son las direcciones IP indicando la dirección del emisor y del receptor.
- **Opciones.** Este campo fue diseñado para permitir que un encabezado IP pueda ser extendido. El campo opciones no es utilizado comúnmente.
- **Datos.** El campo de datos en un paquete IP contiene los segmentos de la capa de transporte, TCP o UDP, que serán entregados al receptor. Aunque en este paquete puede contener otro tipo de datos como mensajes de ICMP.

La Ilustración 5 presenta gráficamente la estructura de un datagrama IPv4.

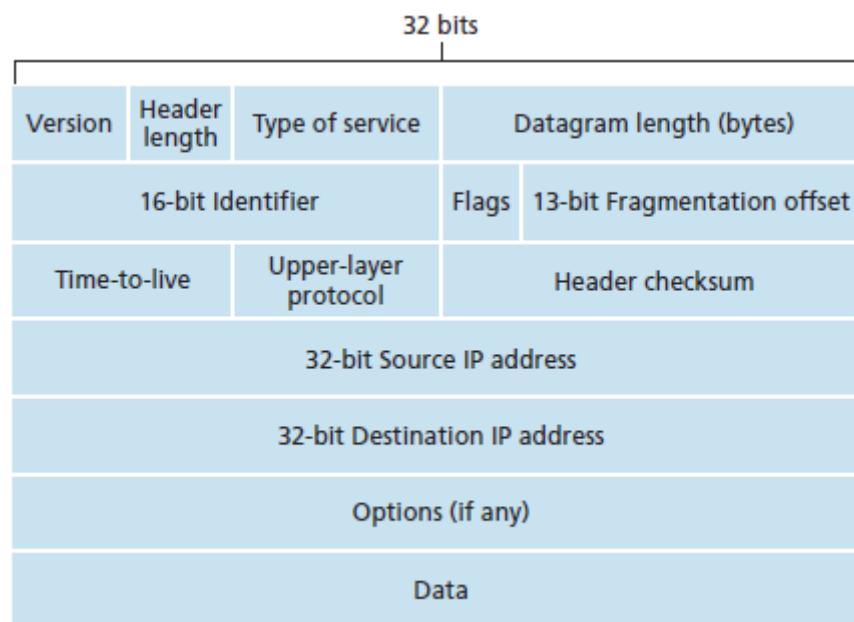


Ilustración 5. Estructura de un datagrama IPv4 (Kurose y Ross 2012)

II.1.4.2 Modos de comunicación IPv4

Dentro de IPv4 existen varias formas que permiten la comunicación entre hosts. Según Tanenbaum (2003) estas son:

- **Direcciones Unicast.** Es una dirección que identifica a un nodo único dentro de una red.
- **Direcciones Broadcast** Es una dirección lógica en la cual todos los dispositivos conectados en un ambiente de red multiacceso pueden recibir paquetes.
- **Direcciones Multicast.** Una dirección multicast es un identificador lógico para un grupo de grupo de hosts en una red.

La Ilustración 6 muestra de forma gráfica el funcionamiento de cada una de las direcciones anteriores. Los nodos en azul son los emisores, mientras que los nodos en verde son los receptores del paquete enviado por dicho emisor.

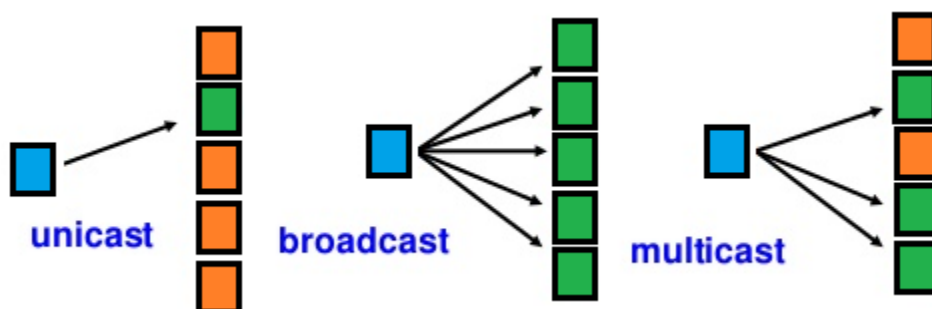


Ilustración 6. Tipos de direcciones

II.1.4.3 Direccionamiento IPv4

IPv4 consta de direcciones de 32 bits las cuales se representan de forma decimal con puntos. La parte decimal de este término proviene de que cada byte (8 bits) de la

dirección de 32 bits está representada con su equivalente en decimal (Odom 2008). La Ilustración 7 muestra una dirección IPv4 en binario y en notación decimal con puntos.

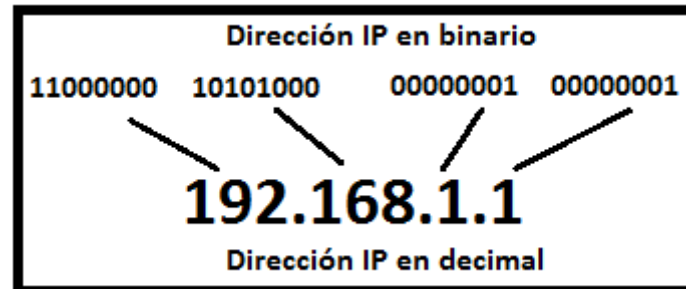


Ilustración 7. Dirección IPv4 en binario y en notación decimal con puntos

Los equipos se conectan a una red mediante una interfaz. Kurose & Ross (2012) definen el término interfaz como: “El límite entre un host y el medio físico”. Igualmente Kurose & Ross (2012) afirman que: “Ya que cada host o ruteador es capaz de enviar y recibir datagramas, IP requiere que cada interfaz de un host y/o ruteador tenga su propia dirección IP. Por lo tanto, una dirección IP está asociada con una interface más que con un host o ruteador que contenga esta interfaz”.

La Ilustración 8 muestra una topología en donde se muestran direcciones IP asignadas a interfaces individuales de hosts y a tres interfaces de un ruteador.

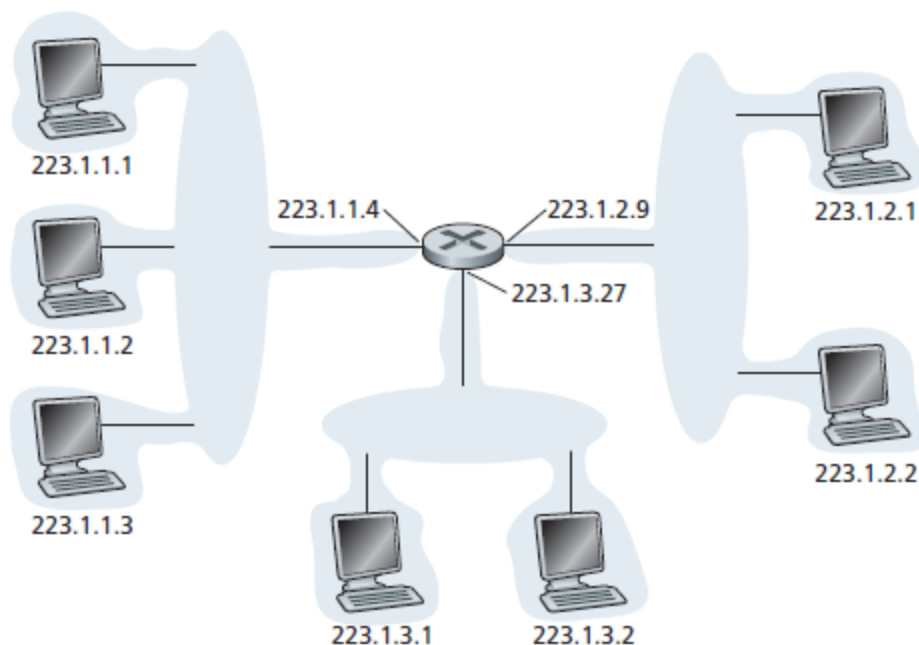


Ilustración 8. Direcciones IP asignadas a interfaces de hosts y de un ruteador (Kurose y Ross 2012)

II.1.4.4 Tipos de direcciones IPv4

Según Odom (2008) existen dos tipos de direcciones IPv4 que se pueden asignar a los hosts dentro de una red. Estas son:

- **Direcciones Públicas.** Son direcciones asignadas por la ICANN. Estas direcciones son únicas a nivel global y pueden navegar en Internet sin necesidad de utilizar mecanismos especiales.
- **Direcciones Privadas.** Las direcciones privadas es un espacio reservado por la IANA que permite a las organizaciones crear su red privada. Este espacio consta de tres bloques. Estas direcciones pueden ser utilizadas por cualquier persona u organización y son necesarios mecanismos especiales como NAT para que estas puedan acceder a Internet. La Tabla 1 muestra los bloques reservados y la cantidad de hosts que se pueden direccionar con ellos.

Bloque	Primera Dirección	Última Dirección	Número de Hosts
10.0.0.0/8	10.0.0.0	10.255.255.255	16,777,216
172.16.0.0/12	172.16.0.0	172.31.255.255	1,048,576
192.168.0.0/16	192.168.0.0	192.168.255.255	65,536

Tabla 1. Bloques reservados para direcciones privadas

II.1.5 Motivaciones para IPv6

En 2011 la IANA otorgo los últimos 5 segmentos /8 a los RIRs para que ellos a su vez los repartieran. Con esta acción se considera que oficialmente no hay bloques IPv4 disponibles (ARIN 2013).

A principios de los 90s la IETF comenzó un esfuerzo por desarrollar un protocolo para substituir a IPv4. La motivación principal para este esfuerzo fue el caer en cuenta que el direccionamiento de 32 bits (IPv4) se comenzaba a terminar. Para responder a esta necesidad de un espacio IP más grande, se desarrolló IPv6. Este nuevo protocolo permitió hacer mejoras a ciertos aspectos de IPv4 basado en la experiencia acumulada de utilizar el anterior protocolo (Kurose & Ross 2012).

II.1.6 IPv6

Los desarrolladores de IPv6 hicieron ciertas adecuaciones y mejoras a este protocolo tomando como referencia las deficiencias de su antecesor IPv4. Según Krajci y Cummings (2013) estas mejoras son:

- **Aumentar la capacidad de direccionamiento.** El tamaño de las direcciones IP se incrementó de 32 a 128 bits. Este incremento asegura que el mundo no se va a quedar sin direcciones IP.

- **Encabezado de tamaño fijo.** En IPv4 el tamaño del encabezado podía ser variable. Para IPv6 este es un campo fijo de 40 bytes, lo cual permite un procesamiento más rápido del datagrama. i
- **Priorización y Marcado de Flujos.** IPv6 tiene capacidad para marcar ciertos flujos de tráfico y darles un trato preferencial.

Las direcciones IPv6 constan de 32 números hexadecimales organizados en 8 grupos de 4 dígitos hexadecimales separados por dos puntos (:) para poder representar una dirección de 128 bits (Odom 2008). Un ejemplo de una dirección IPv6 es el siguiente: 2340:1111:AAAA:0001:1234:5678:9ABC.

IPv6 consta de un prefijo y una máscara de red, esta última ayuda a determinar la longitud del primero. Por ejemplo en la dirección 2340:1111:AAAA:0001:1234:5678:9ABC/64 el prefijo es 2340:1111:AAAA:0001 mientras que el identificador de la red es 2340:1111:AAAA:0001::/64 (Odom 2008).

II.1.6.1 Formato de los Datagramas IPv6

El formato de un datagrama de IPv6 consta de 9 campos, los cuales según el RFC 2460 (1998) son:

- **Versión.** Campo de 4 bits que indica el número de versión de IP. A pesar de poner el valor de “4” en este datagrama, no implica que el paquete sea un paquete IPv4 válido.
- **Clase de Tráfico.** Este campo de 8 bits es similar al campo Tipo de Servicio en IPv4.

- **Etiqueta del Flujo.** Este campo de 20 bits es usado para identificar un flujo de datagramas.
- **Longitud de la Carga.** Este campo de 16 bits es el tamaño total del paquete, incluyendo los encabezados.
- **Siguiente Encabezado.** Campo de 8 bits que especifica el siguiente encabezado. Este campo usualmente contiene el protocolo de transporte utilizado.
- **Límite de Saltos.** Este campo reemplaza al campo tiempo de vida de IPv4. Es un campo de 8 bits y cada vez que se procesa por un ruteador, este decremento su valor.
- **Dirección Origen y Destino.** Estos campos son de 128 bits y contienen las direcciones del emisor y del receptor.
- **Datos.** Este campo contiene los datos a transmitir.

La Ilustración 9 muestra la estructura de un datagrama IPv6:

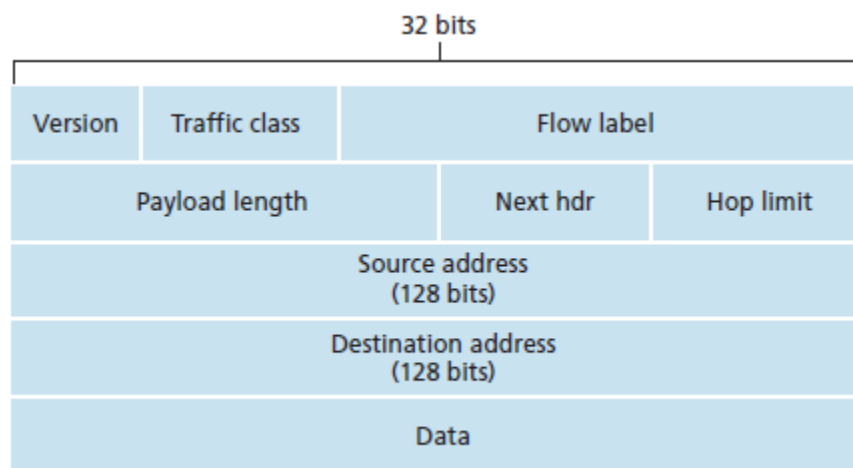


Ilustración 9. Estructura de un datagrama IPv6. (Kurose y Ross 2012)

II.1.6.2 Tipos de Direcciones IPv6

Según Davies (2008) existen tres tipos de direcciones IPv6:

- **Global.** Estas direcciones son el equivalente a las direcciones públicas de IPv4. Estas direcciones son únicas globalmente y pueden acceder a Internet de forma nativa.
- **Link-Local Address.** Estas direcciones son el equivalente a las direcciones APIPA¹⁵ de IPv4 utilizadas por Microsoft para proveer direccionamiento automático en caso de que el host no tenga una dirección IP, ya sea estática o dinámica.
- **Unique Local Address.** Las Unique Local Addresses (ULA) son el equivalente a las direcciones privadas en IPv4 con la diferencia una parte de estas direcciones se genera de forma aleatoria para evitar direcciones duplicadas.

II.1.7 Transición de IPv4 a IPv6

La transición de IPv4 a IPv6 va a ser un fenómeno gradual. Mientras IPv6 no sea el protocolo dominante, es necesario que existan mecanismos que permitan un ambiente de comunicación transparente que soporte ambos protocolos. Sobre estos mecanismos Afifi and Toutain (1999) afirma lo siguiente: “En lo que se refiere a la implementación de IPv6, cualquier mecanismo de interconexión para redes IPv6 e IPv4 se puede separar, pero en donde aplicaciones IPv6 e IPv4 puedan intercambiar información de forma

¹⁵ Automatic Private IP Addressing. Funcionalidad de Windows que provee direccionamiento automático cuando el servidor DHCP no está disponible.

transparente deben ser bienvenidos. Esto permite de utilizar IPv6 en combinación con otros protocolos para un ruteo más flexible.”.

La migración de IPv4 a IPv6 debe ser progresiva y en la medida de lo posible transparente. Nordman y Gilligan (2005) en el RFC 4213 hablan sobre el elemento clave para esta transición: “La clave para una transición IPv6 exitosa es la compatibilidad con la base de equipos IPv4 ya existentes. Mantener la compatibilidad con IPv4 mientras se implementa IPv6 va a acelerar dicha transición”.

II.1.8 Mecanismos de Transición

IPv6 no es compatible con IPv4, estos protocolos no pueden comunicarse entre sí. Mientras los sistemas requieran interoperabilidad con IPv4 e IPv6, se necesitan mecanismos de transición (Frankel, y otros 2010).

Frankel, y otros (2010) mencionan que existen tres mecanismos de transición de una red IPv6 hacia una IPv4. Estos mecanismos son:

- **Dual Stack.** En este método de transición los hosts soportan ambos protocolos, IPv4 e IPv6 simultáneamente.
- **Túnel.** Es la encapsulación de un protocolo dentro de otro. En el contexto de transición hacia IPv6, se hace un túnel de IPv6 sobre IPv4. El protocolo dentro del túnel no es consciente de estar dentro de un túnel y no incurrirá en los recuentos hop mientras que en tránsito.
- **Traducción.** La traducción consiste en transformar paquetes IPv4 o IPv6 en el otro protocolo para que puedan ser ruteados o transmitidos a través de una red. *Network Address Translation – Protocol Translation* (NAT-PT) permite a

dispositivos IPv4 e IPv6 comunicarse entre sí a través de un dispositivo que realice dicha traducción.

II.1.8.1 Dual Stack

El término dual stack significa que un host o un router soporta los protocolos IPv4 e IPv6 al mismo tiempo. Para un host esto quiere decir que tiene direcciones IP de las dos versiones asociadas a sus interfaces, ver *Ilustración 10. Concepto de Dual Stack* Ilustración 10. Mientras que para un router esto significa que debe soportar los protocolos de ruteo tanto para IPv4 como para IPv6 (Odom 2008).

En un ambiente de red con dual stack, un host va a enviar paquetes tanto IPv4 o IPv6 dependiendo del protocolo utilizado por el destino. El dual stack es la técnica que se utiliza con mayor frecuencia en las etapas tempranas de la transición IPv4 a IPv6. (Afifi y Toutain 1999)

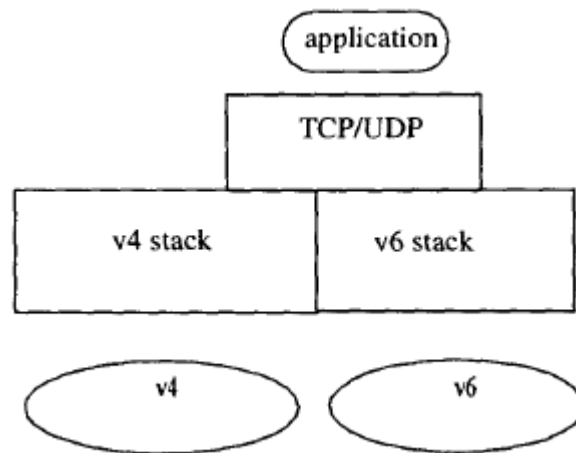


Ilustración 10. Concepto de Dual Stack (Afifi y Toutain 1999)

II.2 Dispositivos Móviles

Según Baz (2009) un dispositivo móvil es: “Un aparato de pequeño tamaño con algunas capacidades de procesamiento, con conexión permanente o intermitente a una red, con memoria limitada, que ha sido diseñado para una función pero puede llevar a cabo otras funciones más generales”.

II.3 Dispositivos Móviles En La Actualidad.

El concepto de dispositivos móviles nace a mediados de los 90s cuando varias compañías comenzaron a desarrollar y comercializar las primeras PDAs. Aunque estas no son consideradas como computadoras móviles, fueron las predecesoras de los smartphones (Hall y Anderson 2009).

En 1999 Research In Motion (RIM) introdujo la Blackberry. Este dispositivo comenzó siendo un *pager*¹⁶, pero rápidamente se convirtió en uno de los dispositivos móviles de mayor uso en el mercado. La Blackberry se diferenció de sus competidores por su teclado QWERTY. En abril del 2008 RIM tuvo un 17% del total de mercado (Hall y Anderson 2009).

Durante varios años Symbian¹⁷ y RIM controlaron el mercado vendiendo sus productos al segmento empresarial como herramientas de trabajo. Pero en enero de 2007 Apple lanza su Smartphone iPhone, quien desde el momento de su lanzamiento estuvo constantemente ganando terreno contra estos (Hall y Anderson 2009)

¹⁶ Dispositivo electrónico utilizado para enviar y recibir mensajes

¹⁷ Sistema Operativo para dispositivos móviles desarrollado por Symbian LTD.

Google en 2005 compra la compañía Android, la cual desarrollaba software para dispositivos móviles (Hall y Anderson 2009). Pero no fue hasta 2007 cuando Google anunció públicamente que Android sería la primera plataforma realmente abierta para dispositivos móviles (Krajci y Cummings 2013).

Según el portal especializado IDC (IDC Research, Inc 2015) el mercado de *smartphones* creció un 13% en el segundo cuarto de 2015. Android es el amplio dominador del mercado con un 82.8% estos datos corresponden al segundo cuarto de 2015. La Tabla 2 hace una comparativa del total del mercado de sistemas operativos móviles en segundo cuarto de los últimos 3 años:

Period	Android	iOS	Windows Phone	BlackBerry OS	Others
2015Q2	82.8%	13.9%	2.6%	0.3%	0.4%
2014Q2	84.8%	11.6%	2.5%	0.5%	0.7%
2013Q2	79.8%	12.9%	3.4%	2.8%	1.2%
2012Q2	69.3%	16.6%	3.1%	4.9%	6.1%

Source: IDC, Aug 2015

Tabla 2. Distribución del mercado mundial de Sistemas Operativos móviles (IDC Research, Inc 2015)

En cuanto a los fabricantes de dispositivos, Samsung es el líder con un 21.4% del total del mercado; estos son datos del segundo cuarto de 2015. La Tabla 3 muestra la cuota de mercado de teléfonos inteligentes en todo el mundo (IDC Research, Inc 2015).

Period	Samsung	Apple	Huawei	Xiaomi	Lenovo*	Others
2015Q2	21.4%	13.9%	8.7%	5.6%	4.7%	45.7%
2014Q2	24.8%	11.6%	6.7%	4.6%	8.0%	44.3%
2013Q2	31.9%	12.9%	4.3%	1.7%	5.7%	43.6%
2012Q2	32.2%	16.6%	4.1%	1.0%	5.9%	40.2%

Source: IDC, Aug 2015

* Motorola figures have been captured under Lenovo.

Tabla 3. Cuota del mercado global de smartphones en el segundo cuarto de 2015 (IDC Research, Inc 2015)

II.3.1

II.4 SISTEMAS OPERATIVOS MOVILES

Según el portal especializado en tecnología Gartner Inc, los tres sistemas operativos móviles con mayor auge en el mercado (hasta enero de 2015) son: Android de Google, IOS de Apple y Windows Phone de Microsoft. La Tabla 4 hace una comparativa de lo anterior y muestra un pronóstico para 2016 (Gartner, Inc. 2015):

Worldwide Device Shipments by Operating System, 2014-2016 (Thousands of Units)

Operating System	2014	2015	2016
Android	1,156,111	1,454,760	1,619,030
iOS/Mac OS	262,615	279,415	298,896
Windows	333,017	355,035	393,256
Others	626,358	380,545	261,155
Total	2,378,101	2,469,755	2,572,338

Shipments include mobile phones, ultramobiles (including tablets) and PCs

Source: Gartner (January 2015)

Tabla 4. Comparativa entre Sistemas Operativos para Móviles (Rivera y Van der Meulen 2015)

Android. Este sistema operativo fue creado por la compañía Android, la cual fue comprada posteriormente por Google en 2005 (Krajci and Cummings 2013). Android es un sistema operativo basado en una versión modificada del Kernel de Linux. El software stack de Android contiene aplicaciones de Java corriendo en una máquina virtual llamada Dalvik. (Butler 2011). La primera versión de Android salió al mercado en 2008. La Ilustración 11 muestra la pantalla principal del sistema operativo Android.

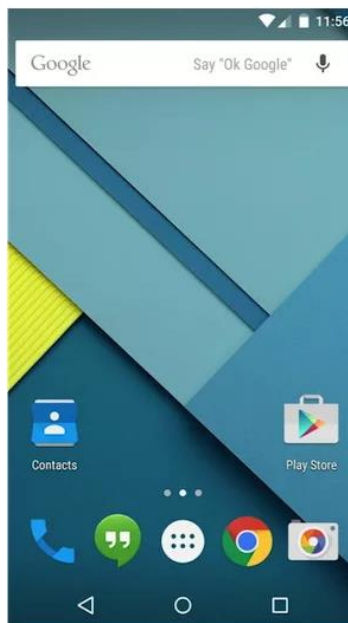


Ilustración 11. Pantalla Principal de Android (Bhantnagar 2015)

Por otro lado, IOS. Este sistema operativo fue diseñado por Apple basado en el sistema operativo OS X. Este sistema operativo fue diseñado en un principio para el iPhone, pero ahora soporta otros dispositivos de Apple como el iPod Touch y el iPad. (Jyothy y Shinto 2013). IOS fue publicado por primera vez en 2007 con la primera versión del iPhone

(Krajci y Cummings 2013). La Ilustración 12 muestra la pantalla principal de un dispositivo Apple con IOS

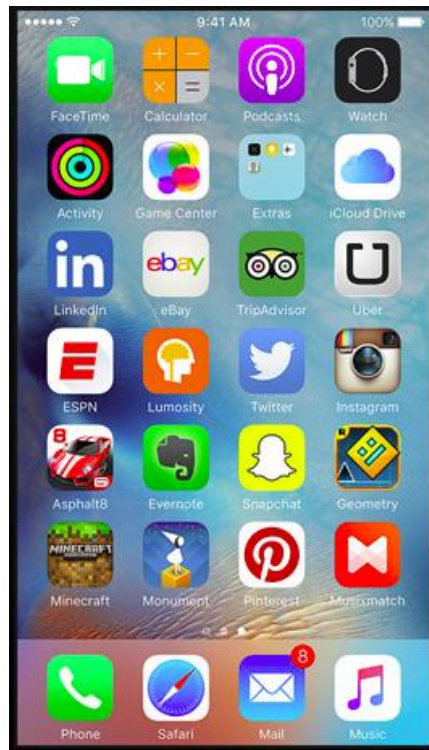


Ilustración 12. Interfaz gráfica de IOS versión 9 (Apple, 2015)

Y finalmente **Windows Phone**. Desarrollado por Microsoft como sucesor de Windows Mobile. Este sistema operativo sale al mercado en noviembre de 2010. Microsoft se ha enfocado en la facilidad de uso y la conectividad con servicios de Windows actuales, tales como Windows Live (Krajci y Cummings 2013). La versión más nueva de sistema operativo (Windows Phone 8) prácticamente simula la interface de una computadora personal con Windows 8.1 (Jyothy y Shinto 2013). La Ilustración 13 muestra la pantalla principal de Windows Phone 8:



Ilustración 13. Página principal de Windows Phone 8 (Winsupersite, 2015)

II.5 GOOGLE

II.5.1 Google INC

Google INC se funda en 1998 en Mountain View California por dos estudiantes de la universidad de Stanford (Larry Page y Sergey Brin). Estos dos crearon un motor de búsqueda que utilizaba enlaces para determinar la importancia de páginas web. Este motor de búsqueda fue bautizado como Google haciendo alusión al término matemático “gugol”. Google Inc. nació en 1998, cuando Andy Bechtolsheim, cofundador de Sun Microsystems, extendió un cheque de 100.000 dólares a esta entidad (Google INC 2015).

Google ofrece una gama de productos que incluyen correo web (Gmail), navegadores Web (Chrome) productos para mercadeo (Google AdWords), plataforma para videos (Youtube), buscador especializado para la academia (Google Scholar), sistemas operativos (Android), smartphones (Nexus) y dispositivos de entrenamiento (Chromecast) por mencionar algunos (Google INC 2015).

Según Forbes (2015): “Google, Inc. se centra en mejorar la forma en que las personas se conectan con la información. Ofrece una gran variedad de servicios y herramientas para anunciantes de todos los tamaños, desde anuncios de texto simples, así como publicidad móvil. La compañía se centra principalmente en las áreas que incluyen la búsqueda, la publicidad, los sistemas operativos, plataformas, la empresa y los productos de hardware”.

II.5.2 Android

Es el sistema operativo más popular en los dispositivos móviles actuales. Está diseñado por Google y está basado en Linux. Es una plataforma *Open Source*, lo que permite que los fabricantes puedan personalizar Android según sus necesidades y utilizarlo en su hardware. Android utiliza el kernel¹⁸ de Linux como su capa de abstracción para el hardware y software, lo que ayuda a tener un mejor manejo de memoria, procesos, opciones de seguridad y de red (Jyothy y Shinto 2013).

La plataforma Android se compone de varias capas que proporcionan un *software stack* completa. Las aplicaciones Android se basan en Java¹⁹ y este factor implica el uso de una máquina virtual con sus ventajas. Android utiliza su propia máquina virtual llamada Dalvik, que interpreta y ejecuta el código portátil de Java. El proceso mencionado anteriormente está optimizado para funcionar en plataformas móviles (Gandhewar y Sheikh 2010).

¹⁸ Kernel es el módulo central de un sistema operativo

¹⁹ Lenguaje de programación orientado a objetos

II.5.2.1 Arquitectura de Android

De acuerdo a Gandhewar y Sheikh (2010) la arquitectura de Android consiste en capas las cuales son:

- **Aplicaciones.** Son las herramientas que los usuarios utilizan para interactuar con el dispositivo. Las aplicaciones en su mayoría están codificadas en Java. Las aplicaciones para Android se pueden obtener a través de la Google Play Store o se pueden instalar a través de una conexión USB y de una tarjeta SD. (Krajci y Cummings 2013)
- **Marco de Aplicación.** Android ofrece a los desarrolladores la capacidad y las herramientas para crear extensas y ricas aplicaciones interactivas, gráficos para los usuarios. Este marco de aplicación está diseñado para agregar estas nuevas aplicaciones a la Google Play Store. Los desarrolladores tienen acceso a las mismas API²⁰ que se utilizan dentro de las aplicaciones principales, así a casi todas las librerías²¹ de Java existentes (Krajci y Cummings 2013)
- **Librerías.** Esta capa se divide en dos partes:
 - **Librerías Nativas.** Librerías escritas en C/C++ que son llamadas a través de una interface de Java. (Gandhewar y Sheikh 2010)
 - **Android Runtime.** Dentro del Android Runtime existen dos componentes principales: las bibliotecas del núcleo de Java que Android ofrece y la máquina virtual Dalvik. Esta máquina virtual es la de implementación que

²⁰ La interfaz de programación de aplicaciones

²¹ Suite de datos y código de programación para desarrollar programas y aplicaciones

hace Google del lenguaje de Java, la cual está optimizada para ser utilizada en dispositivos móviles. (Krajci y Cummings 2013)

- **Kernel de Linux.** Android está basado en Linux con un kernel versión 2.6 para acceder a los servicios del sistema central tales como: seguridad, gestión de memoria, administración de procesos, funciones de red y controladores de dispositivos (drivers²²). El kernel también actúa como una capa de abstracción entre el hardware y el resto de la software stack (Gandhewar y Sheikh 2010).

La Ilustración 14 muestra de forma gráfica la arquitectura del sistema operativo Android.

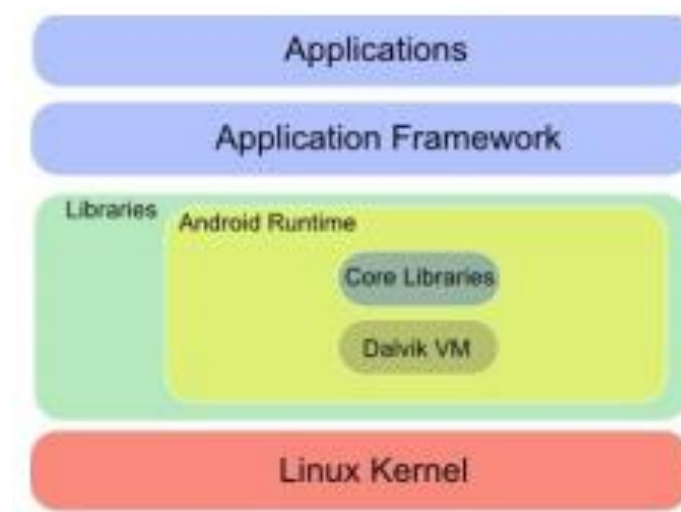


Ilustración 14. Arquitectura de Android (Gandhewar y Sheikh 2010)

II.5.3 Android Compatible

Sobre los dispositivos que son Android Compatible, Google (Google Inc. 2015) establece lo siguiente:

²² Elemento de software utilizado en los sistemas operativos para interactuar con el hardware

Android está diseñado para correr en diferentes tipos de dispositivos que van desde teléfonos, tabletas y televisiones. Al ser un sistema operativo Open Source cualquier fabricante puede construir un dispositivo que pueda correr Android. Pero, el dispositivo es Android Compatible solamente si puede correr aplicaciones escritas para el ambiente de ejecución de Android

Como un desarrollador de aplicaciones no es necesario preocuparte si un dispositivo es Android Compatible porque solamente estos últimos son incluidos los que están incluidos en la Google Play Store. De esta manera se puede asegurar que quien instale una aplicación usando la Google Play Store lo hará en un dispositivo compatible.

Para que un dispositivo se considere Android compatible, tiene que seguir el siguiente proceso:

- **Obtener el código fuente de Android.** Este es el código fuente de la plataforma Android que se va a instalar en el dispositivo.
- **Cumplir con el Documento de Definición de Compatibilidad** Compatibility Definition Document, CDD por sus siglas en inglés. Es un documento publicado por Google en el cual se listan los requerimientos que un dispositivo debe cumplir para ser considerado Android Compatible. Esos requerimientos son tanto de hardware como de software.
- **Pasar la Suite de pruebas de Compatibilidad.** CTS por sus siglas en inglés. En la sección correspondiente se explicará con más detalle

Según una vez cumplidos los tres pasos anteriores, el dispositivo se considera Android Compatible (Google Inc. 2015).

II.5.4 Compatibility Test Suite

El *Compatibility Test Suite* (CTS), explicado en el portal de Android ([https://source.android.com/compatibility/cts](#)), es un set de pruebas automatizadas que consiste de dos componentes de software principales:

- Las pruebas del CTS ejecutadas en la máquina de escritorio utilizando tradefed²³
- Las pruebas individuales ejecutadas directamente en el dispositivo de prueba.

Las pruebas del CTS cubren las siguientes áreas para asegurar compatibilidad:

- **Pruebas de Firma.** Esta prueba consiste en comparar las firmas de todas las APIs públicas y compararlas contra las existentes en el dispositivo.
- **Pruebas del API de la Plataforma.** En esta prueba se valida que las librerías y sus objetos tengan el comportamiento esperado en el dispositivo.
- **Pruebas de Dalvik.** Estas pruebas se enfocan en verificar que los ejecutables para Dalvik funcionen de acuerdo a lo esperado.
- **Modelo de Datos de la Plataforma.** El objetivo de estas pruebas es verificar que los métodos y funciones expuestos hacia el desarrollador a través del SDK²⁴ estén realmente disponibles.
- **Intención de la Plataforma.** Las pruebas de Intención de la Plataforma verifica que las llamadas a aplicaciones externas funcionen según lo documentado en el SDK.
- **Permisos de la Plataforma.** Verificar los permisos de la plataforma.

²³ Aplicación de Google escrita en Java que se ejecuta en la computadora donde se está haciendo el desarrollo de la aplicación y se comunica con uno o varios dispositivos Android.

²⁴Set de herramientas de programación para desarrollar aplicaciones en una plataforma específica

- **Recursos de la Plataforma.** En estas pruebas se verifica que la plataforma maneje correctamente los recursos

II.6 INTEL

II.6.1 INTEL Corporation

Krajci y Cummings (2013) hacen la siguiente reseña sobre la historia de INTEL:

INTEL es una de las empresas de manufactureras de semiconductores más antiguas del mundo y es conocido por la creación de tecnologías innovadoras y funcionales en el hardware de la computadora, así como para las industrias relacionadas.

La compañía fue fundada por Bob Noyce y Gordon Moore en 1968. Arthur Roca, un capitalista de riesgo, apuntaló esta empresa con una inversión inicial de \$ 10,000 y una contribución posterior de \$ 2.5 millones de dólares

Intel lanzó sus dos primeros productos en 1969: la memoria de acceso aleatorio bipolar Schottky 3101 y el 1101, semiconductor de óxido de metal primero del mundo (MOS). El primer procesador de Intel fue lanzado en 1971, y fue llamado el 4004.

En 1978 INTEL lanza su primer procesador, el 8086, construido originalmente como una extensión de 16 bits experimental del microprocesador de 8 bits Intel 8080. El 8086 fue el procesador que impulsó la "IBM PC" y todos sus clones. El término x86 se derivó de los sucesores de los 8086, todo lo cual terminó en "86." En 1985, Intel continuó la arquitectura x86 con el Intel 80386, el primer procesador de 32 bits. No fue hasta 2005, con el lanzamiento del Pentium 4, que los procesadores x86 de 64 bits lleguen al mercado.

La última serie de procesadores de INTEL con arquitectura x86 es conocida como INTEL Core i-series. Esta serie es compatible con operaciones de 64 bits y se centra en el rendimiento y la velocidad. Todos los procesadores de esta familia soportan la tecnología hyperthreading²⁵ y cuentan con múltiples núcleos²⁶, que permiten el procesamiento concurrente. En paralelo a los procesadores Core i-series INTEL desarrolló la serie Atom, la cual está diseñada para dispositivos móviles y también está basada en la arquitectura x86.

La arquitectura x86 original se ha diversificado añadiendo nuevas especificaciones, y ha sido modificada para funcionar en factores de forma²⁷ más pequeños. Lo anterior ha permitido que esta arquitectura se siga utilizando en una amplia gama de dispositivos. La incorporación de Android en x86 es sólo otro paso adelante para INTEL.

Gracias a la difusión y uso de la arquitectura x86 en diversas tecnologías como en servidores, laptops, *smartphones*, y *tablets* por mencionar algunas, se ha creado herramientas, aplicaciones, *frameworks* y bibliotecas para el desarrollo de software específicas para las plataformas x86.

II.6.2 Procesadores INTEL en plataformas Móviles.

La línea de procesadores Atom se ofrece en dispositivos móviles. Dispositivos típicos incluyen laptops, netbooks, tablets, televisores y teléfonos inteligentes. El procesador

²⁵ Tecnología propietaria de INTEL para el manejo de hilos de programación simultáneos.

²⁶ Unidad de procesamiento que puede leer y ejecutar instrucciones de programas

²⁷ En computación un factor de forma, o form factor, se refiere al tamaño de un dispositivo de cómputo

Atom tiene un balance entre rendimiento y uso de energía, lo cual permite alargar la vida de la batería (Krajci y Cummings 2013).

Atom es un procesador complemente compatible con x86²⁸, lo cual significa que funciona con aplicaciones como juegos y navegadores desarrolladas para los chips x86 de computadoras y servidores con esta misma arquitectura (Smith 2008).

El tamaño y el bajo consumo de energía del Atom son dos características importantes de este procesador. Atom consta de 47 millones de transistores, con un tamaño de 25 milímetros cuadrados, consume 2 watts cuando opera a máxima velocidad ,100 miliwatts a bajas velocidades y 200 miliwatts en promedio al ejecutar diversas aplicaciones (Smith 2008).

II.7 METODOLOGÍA DE IMPLEMENTACIÓN DE DUAL STACK NIST

Así como Nordman y Gilligian, Frankel y otros (2010) de igual forma afirman que la transición de IPv6 debe ser gradual y con la menor disrupción posible. Estos últimos, con el aval de la NIST³¹, proponen una serie de directrices para asegurar una transición segura y exitosa hacia IPv6. Esta implementación debe seguir las siguientes fases:

- **Fase de Iniciación.** En esta fase se realiza el levantamiento de requerimientos. Es muy importante para la organización conocer su ambiente tecnológico actual antes de implementar IPv6. Esta etapa permite corregir problemas existentes con IPv4, simplificar el direccionamiento y/o el ruteo. Se debe analizar

²⁸ Arquitectura de procesadores desarrollada por Intel. Esta es derivada del procesador 8086

³¹ National Institute of Standards and Technology. Agencia federal de los Estados Unidos que promueve y mantiene estándares de medición. Cuenta con programas para incentivar la ciencia y la industria para adoptar y crear dichos estándares.

cuidadosamente las aplicaciones actuales y su compatibilidad con IPv6; y en caso de no contar con ella, planear mecanismos de coexistencia. Durante esta etapa la organización debe verificar cuales dispositivos dentro de su infraestructura careen de soporte para IPv6; y con base en lo anterior decidir que equipos deben ser reemplazados.

- **Fase de Desarrollo.** Durante esta fase se toman los requerimientos obtenidos en la etapa inicial y con base en lo anterior se desarrolla la arquitectura IPv6. Durante esta etapa la organización debe planear un piloto utilizando IPv6 en el cual se probaran y evaluaran las configuraciones y funcionalidad de IPv6 dentro de la red. A lo largo del periodo piloto es necesario y recomendable realizar pruebas de desempeño de la red, planear estrategias para mitigar posibles problemas así como realizar una valoración de riesgos de seguridad en el ambiente. Al finalizar la fase de desarrollo, la organización deberá haber generado los siguientes documentos: Arquitectura Empresarial, Plan de Asignación de Direcciones, Plan de Administración de direcciones, Plan de Ruteo, Plan de Entrenamiento, Plan de Seguridad y Plan de Coexistencia.
- **Fase de Implementación.** La fase de implementación se encarga de la instalación, configuración, túneleo y demás mecanismos de transición para IPv6 en los equipos de red. Durante esta etapa se definirá cual escenario se ajusta mejor al ambiente; los escenarios son: Implementación de IPv6 Generalizada³² (Pervasive IPv6 deployment) o Implementación de IPv6 Dispersa³³ (Sparse IPv6

³² Este tipo de implementación se utiliza cuando los equipos soportan tanto IPv4 como IPv6 y no se necesitan métodos alternos para trabajar con ambos protocolos en paralelo

³³ Esta implementación se utiliza cuando los equipos no soportan nativamente IPv6

deployment). Sin importar el tipo de escenario la implementación de IPv6 se hará por fases.

- **Fase de Operación/Mantenimiento.** Esta fase inicia simultáneamente con la fase de Implementación. Durante la etapa de Operaciones el foco de atención es asegurar la operación segura del ambiente mixto de IPv4 e IPv6. Una de las tareas más complejas de esta fase es la de mantener ambos ambientes sincronizados. Cualquier cambio hecho en IPv4 debe reflejarse en el ambiente IPv6 y viceversa.
- **Fase de Disposición.** Migrar completamente de IPv4 a IPv6 generalmente trae consigo que haya equipo de red que se tenga que desechar y retirar del ambiente por diversas razones. La principal es que no soporta IPv6 de forma nativa o que es obsoleto. Durante esta etapa la organización planea que equipo hay que retirar y como deshacerse de el de una forma segura y que no comprometa información confidencial.

III. MARCO METODOLÓGICO

III.1 De la Investigación

Para el desarrollo de esta investigación se utilizó el paradigma hermenéutico-interpretativo de la investigación. Lo anterior dado que los postulados planteados por Vargal Beal (2012) para este paradigma son acordes al trabajo. Estos postulados son:

- 1) La realidad es subjetiva
- 2) Se plantea la implicación del sujeto con el objeto
- 3) La realidad es estructural y/o sistémica
- 4) La realidad es compleja

5) La realidad es interpretable.

Uno de los métodos más importantes de este paradigma, y el utilizado en este trabajo, es el de investigación-acción. Algunas de las técnicas que se utilizaron fueron: la observación directa, la entrevista profunda, la entrevista semi-estructurada y grupo en conversación principalmente.

III.2 De la adecuación del laboratorio de INTEL en Rumania para el soporte de IPv6

El diseño e implementación de este proyecto se realizó con base en la experiencia y conocimientos previos del autor. El desarrollo se realizó en tres grandes fases: La fase análisis en la cual se recabaron los requerimientos del grupo de negocios, se analizaron las necesidades del cliente, sus expectativas y se identificaron las restricciones para la implementación; la segunda fase fue el diseño de la solución y las pruebas de laboratorio del mismo; en esta etapa se probaron los diferentes diseños propuestos para evaluar la mejor solución y finalmente la fase de implementación en la cual se adecuó el laboratorio utilizando el diseño elegido en la fase anterior.

A lo largo de la fase de análisis existió un intercambio de correos y diversas conferencias en los cuales se requería diferente información y se proporcionaban avances del proyecto. De igual forma se llevaron a cabo diferentes juntas con los involucrados para aclarar diversos puntos y resolver dudas.

Durante la fase de pruebas de laboratorio el autor se documentó con diversas fuentes para tomar diseños de red que cumplieran con las mejores prácticas para después

hacerles las adecuaciones necesarias y hacer las implementaciones de prueba en un ambiente de laboratorio.

Para la fase de implementación se trabajó con el líder de proyecto por parte del cliente y los dueños de la infraestructura de red para explicarles el diseño, su funcionalidad, las implicaciones y finalmente para acordar tiempos de implementación y prueba.

IV. DESARROLLO

El desarrollo de este proyecto se llevó a cabo en tres grandes fases: análisis, diseño e implementación. Las siguientes secciones describen lo realizado durante el proyecto y los resultados obtenidos en cada fase.

IV.1 Inicio del Proyecto

El proyecto inicia el **20 de Mayo de 2014** cuando Andrei I. (*líder técnico de Desarrollo*) levanta un ticket con la solicitud de habilitar el protocolo IPv6 dentro del laboratorio de desarrollo en Rumania, el Anexo 1 es el correo enviado por Andrei I. con esta petición. Su equipo estaba teniendo retrasos en la certificación de productos que estaban diseñados para trabajar con la plataforma operativa Android. Las pruebas requeridas por Google para certificar un dispositivo como Android Compatible requerían tener una infraestructura de red que soportara los protocolos IPv4 e IPv6 (*dual stack*).

El **28 de mayo de 2014** al no obtener respuesta sobre su petición, Andrei I. envía un correo a los encargados de la red a nivel Europa para pedir soporte. Esta escalación fue atendida por el Rene B. (*ingeniero de soporte a redes*) quien se encargó de contactar a Daniel K. (*dueño del portafolio de WAN*) para aclarar la situación y establecer los pasos

a seguir ya que no existía un proceso definido para este tipo de implementaciones por ser única.

Este último recibe esta comunicación e incluye al Blaine B. (*especialista en redes*) en las comunicaciones. Blaine estuvo trabajando en definir un set de pruebas de IPv6 para certificar la compatibilidad de este protocolo con los equipos de red corporativos - específicamente con los equipos de seguridad Cisco ASA -. Durante este periodo Blaine trabajó con ingenieros del equipo de NSE (*Network Services Engineering*) para realizar estas pruebas. El Blaine contacta a Mike M. (*gerente de NSE*) para averiguar el avance de las pruebas de IPv6 en estos dispositivos. Las pruebas anteriores no fueron realizadas ya que Mark M. quien era el ingeniero asignado para realizarlas, dejó la compañía sin haberlas ejecutado.

Mike M. decide involucrar en este proyecto a tres personas de su equipo en Guadalajara. Estos ingenieros son Marco C., Rodrigo P. y Juan Carlos L. El **6 de junio de 2104** los tres anteriores tuvieron una junta donde acordaron que Juan Carlos sería el encargado de realizar este proyecto en su totalidad.

IV.2 Fase de Análisis

Dentro de la fase de análisis se buscó entender las actividades que los equipos de desarrollo realizaban, cuál era la necesidad para una implementación de IPv6 y la urgencia que esta tenía para la unidad de negocios.

En primera fase tuvo dos objetivos principales: identificar a los involucrados claves en el proyecto y recabar los requerimientos y expectativas del cliente para esta implementación.

IV.2.1 Recabar Requerimientos

Fueron necesarias varias juntas para comprender en su totalidad el proyecto, entender las necesidades y expectativas del equipo de Andrei y poder identificar a los individuos clave para esta implementación. Los requerimientos de parte del cliente fueron:

- Tener acceso desde el laboratorio hacia Internet con IPv6
- Las reglas de acceso desde y hacia internet con IPv6 deben ser las mismas que las que existen en el laboratorio para IPv4
- Los desarrolladores deben poder acceder a la red con IPv6 del laboratorio tanto por cable como inalámbricamente, de la misma forma que lo hacen para la red IPv6.

IV.2.2 Expectativas del cliente

El cliente desea tener acceso inalámbrico a Internet en el laboratorio a través de IPv4 e IPv6 para poder realizar las pruebas requeridas por el CTS de Google para la validación de dispositivos con sistema operativo Android

IV.2.3 Topología IPv4 del laboratorio

El primer paso para comenzar a realizar diseño para la implementación, fue entender la topología actual del laboratorio y restricciones de la implementación para IPv4. Este laboratorio es un ambiente que consta de dos *switches* interconectados entre ellos, dos *Access Point* para proveer conectividad inalámbrica hacia el laboratorio y un *firewall* el

cual es el dispositivo frontera. La conexión a internet se hace a través de un proveedor local en Rumania (Idilis). La Ilustración 15 muestra un diagrama de la topología del laboratorio.

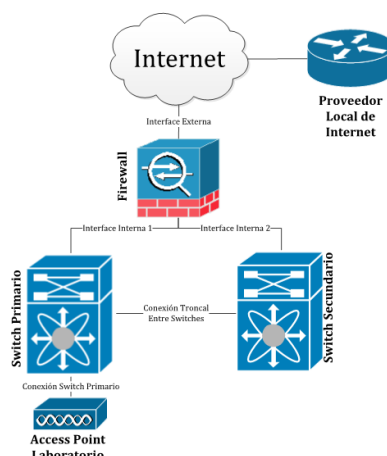


Ilustración 15. Diagrama de red del laboratorio de INTEL Rumania

El laboratorio está conformado por cuatro redes:

- La red externa. o WAN, que conecta al laboratorio con el ISP; esta tiene un direccionamiento público. El firewall hace un NAT³⁴ para permitir a los clientes internos navegar.
- La red de administración es una VPN desde el firewall hacia INTEL. Esta red está asociada con la VLAN³⁵ A.
- La red interna; red en la cual se encuentran diversos servidores y dispositivos de prueba. Esta red se encuentra sobre la VLAN B y tiene un direccionamiento IP privado.

³⁴ *Network Address Translation*. Estándar que permite enmascarar una o varias IPs (generalmente privadas) contra otra IP (generalmente pública)

³⁵ *Virtual LAN* - Estándar para dividir un switch lógicamente en varios dominios de *broadcast*

- La cuarta red se encuentra detrás del Access Point (AP). En esta red es donde se lleva a cabo la validación de los equipos y al igual que la red interna tiene un direccionamiento privado.

La Ilustración 16 muestra la distribución de redes dentro de laboratorio.

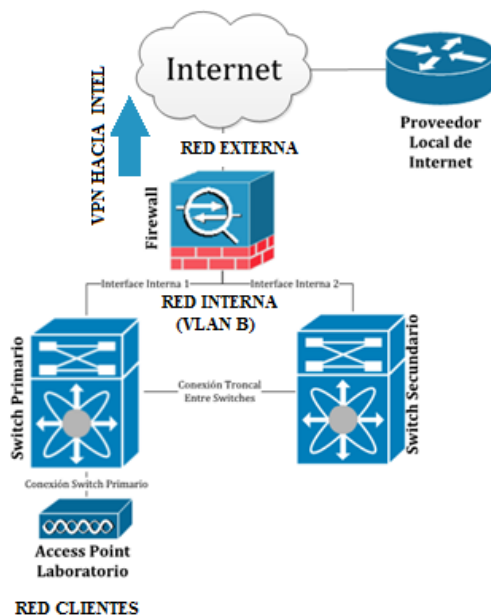


Ilustración 16. Distribución de redes dentro del laboratorio

Por la naturaleza del laboratorio y las pruebas que se llevan en él, las redes interna (VLAN B) y de clientes se encuentran completamente aisladas de la red corporativa. Cuando un usuario necesita realizar pruebas que requieran el uso de las redes del laboratorio, este debe desconectarse de la red corporativa y conectarse a la del laboratorio. Por política corporativa no está permitido el *multihoming*³⁶.

El propósito de la red de administración es el de acceder remotamente, respaldar, monitorear y configurar los equipos de red dentro del laboratorio. No hay conectividad

³⁶ Dispositivo o computadora que se encuentra conectado a más de una red.

alguna entre la red de administración con las redes internas del laboratorio. El firewall se administra por la consola de Cisco CSM³⁷. Todos los cambios de configuración deben realizarse por medio de esta herramienta.

El firewall es el encargado de hacer el ruteo entre Internet y la VLAN B. De igual forma este dispositivo hace las veces de servidor DHCP³⁸ para esta red. Las reglas de acceso no son muy restrictivas dentro de este ambiente. Este dispositivo cuenta con una versión de sistema operativo versión 8.X.

Dentro de la red de clientes, el AP es el Gateway y servidor DHCP. La interface WAN de este equipo se conecta a la VLAN B y recibe direcciones IP del firewall. De igual forma el AP enmascara el tráfico de los equipos conectados a su red interna (red clientes) mediante un NAT y lo reenvía hacia al firewall quien es el dispositivo final para salir a Internet. La red de clientes no está conectada a los *switches* del laboratorio. Por cada Access Point existente en el laboratorio, había una red de clientes independiente. Al momento de la implementación existían dos *Access Points* marca D-Link modelo DIR-600.

IV.2.4 Restricciones del Laboratorio

A continuación, se listan las restricciones encontradas para realizar la implementación de IPv6 en el laboratorio:

- El ancho de banda del enlace con el proveedor no se va a incrementar

³⁷ Cisco Security Manager – Herramienta para administrar de forma centralizada dispositivos de red Cisco

³⁸ *Dynamic Host Configuration Protocol* – Protocolo cuya función es la de repartir direcciones IPs a dispositivos en la misma red.

- Todas las configuraciones hechas al firewall se deben realizar a través del CSM
- El soporte en sitio solamente está disponible de 9 a 6 tiempo local (GMT +2)
- La ventana de mantenimiento autorizada es de máximo 12 horas
- El sistema operativo actual del firewall no puede ser actualizado. Esta versión es la autorizada por el departamento de IT de INTEL.
- La topología del laboratorio puede ser modificada siempre y cuando no se afecte la funcionalidad de la red IPv4.

IV.3 Fase de Diseño

En esta fase se evaluaron diferentes alternativas para la implementación del proyecto. De igual forma se hicieron diversas pruebas de laboratorio para corroborar el funcionamiento esperado para de la solución propuesta.

A continuación se listan las soluciones que se analizaron y probaron dentro del laboratorio como posibles opciones para la implementación y un análisis de porque fue aceptada o rechazada.

IV.3.1 Firewall Transparente

La primera solución que se pensó fue la de un firewall transparente. Este es una forma de operación del dispositivo en la cual el firewall no hace ruteo de paquetes entre redes, se convierte en un dispositivo intermedio entre el ruteador y la red. En este modo el

equipo extiende el dominio de broadcast³⁹ de la red. La Ilustración 17 describe una topología de un firewall transparente.

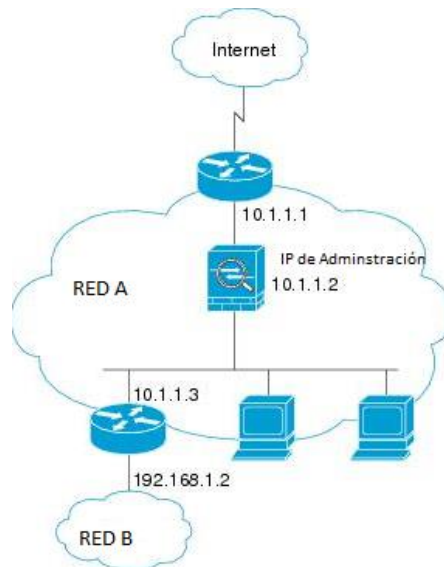


Ilustración 17. Topología de red con un firewall transparente

Se pensó en esta solución por el aparente manejo más sencillo de la red. Se pensaba en extender la subred de IPv6 desde el proveedor hasta el laboratorio de forma transparente a través del firewall. En este mismo dispositivo se implementarían las reglas de acceso y no habría que configurar ruteo adicional.

Esta solución fue desechada por las siguientes razones:

- El cambio a modo transparente implicaba la pérdida de la configuración actual, lo cual traería re trabajos, soporte local y pérdida de conectividad al dispositivo.

³⁹ División lógica de una red de computadoras en la cual los dispositivos se pueden comunicar entre sí sin necesidad de un equipo de capa 3

- El modo transparente se aplica a todo el dispositivo, esto implicaría tener que modificar la topología de la red IPv4. Lo anterior no era opción

IV.3.2 IPv6 subred única con DHCPv6 en el firewall

Esta opción consistía en tener una sola red IPv6 en el laboratorio en donde el firewall sería el servidor DHCPv6; esta topología sería una réplica de la topología IPv4 existente en el laboratorio. La Ilustración 18 es un ejemplo de esta topología.

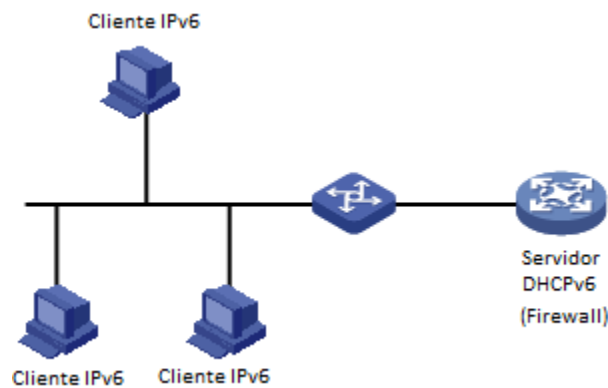


Ilustración 18. Firewall haciendo la función de servidor DHCPv6

La conectividad hacia el ISP se haría con una red punto a punto con direcciones ULA⁴⁰ con una ruta por default en el firewall hacia el proveedor y este último tendría la ruta de regreso hacia la red asignada para el laboratorio. La red asignada fue una red /64.

Esta topología presenta las siguientes ventajas:

- No se requería utilizar dispositivos extra para tener IPv6 en la red
- Ambas redes, IPv4 e IPv6, tendrían la misma topología haciendo más sencilla la administración del laboratorio.

⁴⁰ Unique Local Addresses. Direcciones privadas para IPv6

- La red sería muy escalable. Solamente con poner los puertos del *switch* en la VLAN adecuada se podría tener acceso IPv6 tanto vía cable, como inalámbrico, conectando un *Access Point* a ese puerto.

A pesar de las ventajas de esta propuesta; no fue elegida por las siguientes limitaciones encontradas:

- La versión de IOS 8.2 para el Cisco ASA no soportan el rol de servidor DHCPv6. Solamente el de Servidor Relay ⁴¹ de DHCPv6
- Utilizar esta solución implicaría que uno de los *Access Points* tuviera el rol de servidor DHCPv6. Esto no es el escenario ideal ya que los equipos dentro del laboratorio no son de clase empresarial y no son tan confiables. Por otro lado, los *Access Points* no están monitoreados y en caso de una falla tomaría más tiempo detectarla y corregirla.
- Si se deseara utilizar esta propuesta sería necesario agregar un equipo que hiciera las funciones de servidor DHCPv6. Esto pudiera ser posible, pero habría que discutirse con el departamento de IT y con el gerente del grupo. Uno para que acepte administrar un dispositivo nuevo y el otro para que autorice y fondee la compra.

IV.3.3 IPv6 subred única con SLAAC en el firewall

Este enfoque idéntico al anterior en términos de topología de red y funcionalidad, pero utilizando SLAAC⁴³ en lugar de DHCPv6. SLAAC es un mecanismo en donde el cliente

⁴¹ Es un equipo que se encarga de reenviar las peticiones de red hacia otro.

⁴³ Stateless Address Autoconfiguration – Autoconfiguración Automática de Direcciones. Mecanismo similar a DHCP para asignar direcciones IPv6

utilizando su dirección MAC y el prefijo de la red obtenido a través de un RA⁴⁵ genera su propia dirección. En este método no se tiene registro de cuales direcciones se encuentran asignadas a cuales equipos.

La Ilustración 19 muestra una topología ejemplo en la cual el router anuncia el prefijo de la red hacia los equipos H1, H2, H3 y H4 a través de un RA.

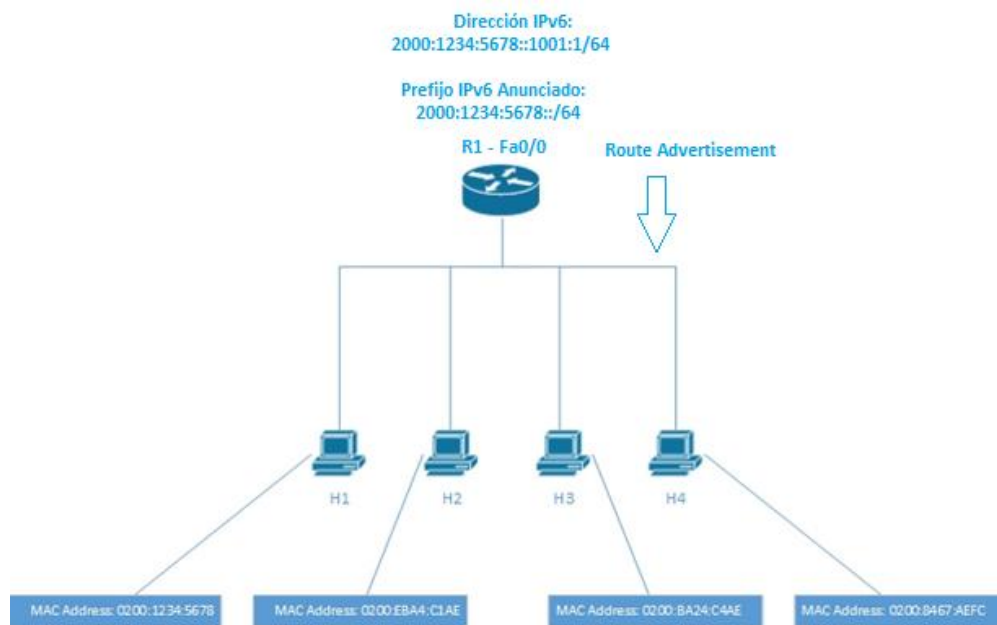


Ilustración 19. Router anunciando el prefijo de la red a través de los RA

Para probar esta tecnología se montó un laboratorio que consistía de los siguientes dispositivos:

- Servidor VMWare ESX. El propósito de este servidor era de tener 4 máquinas virtuales (MV), 2 de ellas simularían clientes, una de ellas haría las funciones de un servidor web en Internet, mientras que la restante tenía instalado el CSM.

⁴⁵ Route Advertisement – Aviso de Ruta. Mensaje IPv6 que envían los gateways IPv6 con el prefijo de la red.

- Cisco ASA 5505 con IOS 8.2. Aunque este dispositivo no era el mismo modelo que el del laboratorio, tenía la misma versión de sistema operativo y lo anterior no afectaba la funcionalidad.
- Cisco Catalyst 4500. Este switch solamente servía para dar conectividad al ambiente.
- Access Point D-Link Dir-600. Este dispositivo se instaló para probar el acceso inalámbrico a la red de prueba utilizando IPv6.

La configuración que se realizó fue la siguiente:

- 2 vlans en el switch.
 - VLAN A simulaba la red interna del laboratorio
 - VLAN B simulaba el enlace con el proveedor
- 2 redes IPv6 en el firewall.
 - La red interna se asoció a la interface interna del equipo. SLAAC se habilita de forma automática en la interface al configurar una dirección IPv6.
 - La interface externa se configuró como un enlace punto a punto con el servidor
 - El firewall era el Gateway de la red.
- SSID de prueba en el Access Point
 - Se configuró una red Wireless con seguridad utilizando WPA2+PSK. Este es el esquema de seguridad que se utiliza en el laboratorio en Rumania.
- La configuración de las máquinas virtuales fue la siguiente:

- Se instaló Ubuntu Server en el servidor web. De la misma forma se instaló Apache como servidor HTTP y se configuró el direccionamiento IPv6. La puerta de enlace de este servidor era la IP de la interface externa del firewall. Se deshabilitaron todas las funciones IPv4. Este equipo se conectó al switch en la VLAN B.
- Para la maquina cliente 1, se utilizó Microsoft Windows 8.1 como sistema operativo.
- En la segunda máquina virtual se instaló Ubuntu como cliente. Al igual que el cliente 1, esta máquina virtual estaba asociada a la VLAN A.
- El Gateway de ambos equipos virtuales era la IP de la interface interna del ASA.
- Para esta prueba se configuró una regla de acceso que permitiera todo el tráfico entre ambas redes. Esto con el fin de facilitar el desarrollo de la prueba.

Las siguientes ilustraciones describen la topología del laboratorio tanto a nivel físico como a nivel lógico.

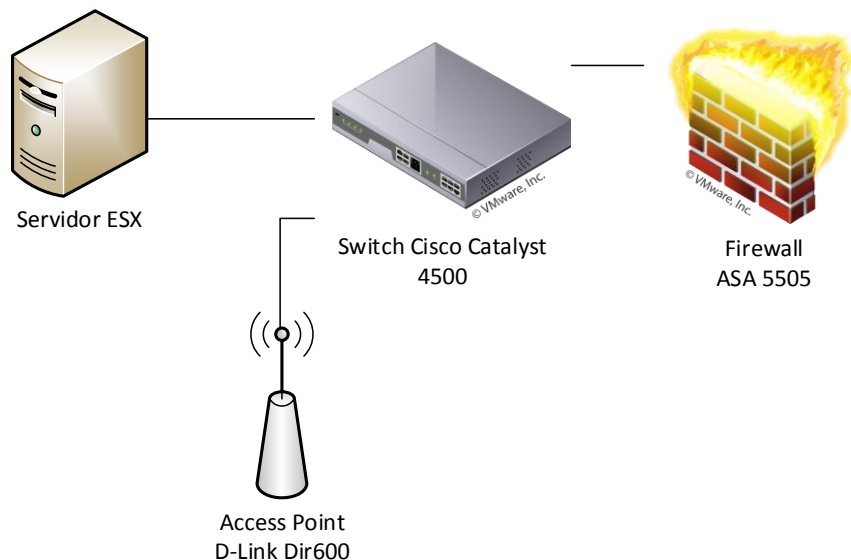


Ilustración 20. Topología física del laboratorio

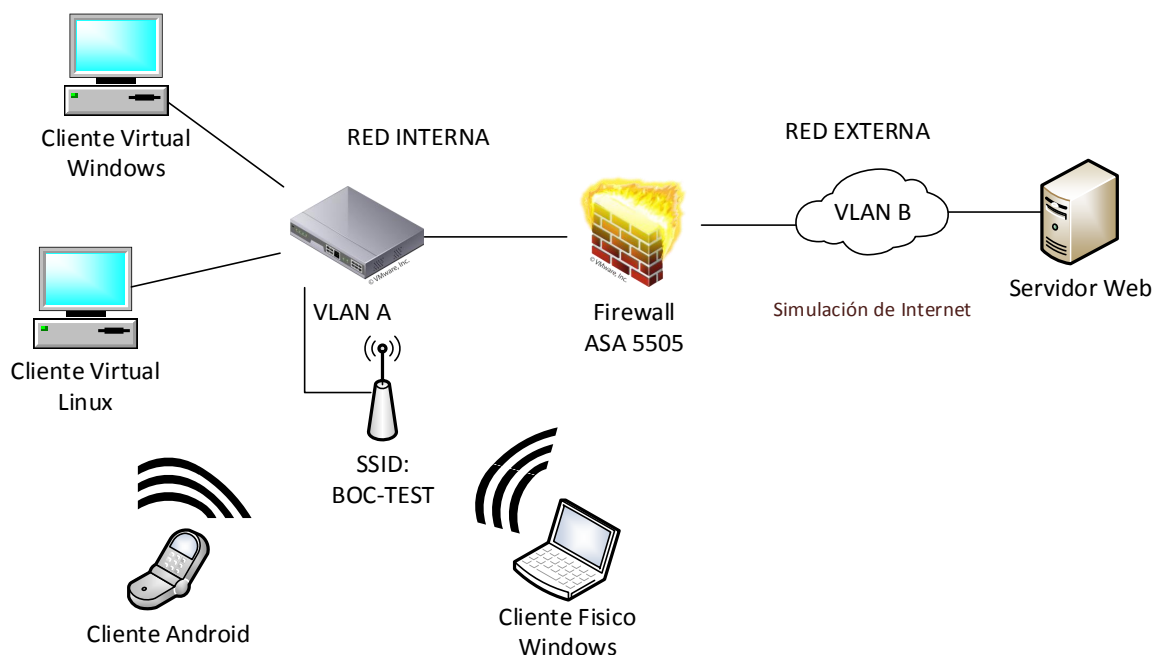


Ilustración 21. Topología lógica del laboratorio

Los resultados de las pruebas fueron negativos en general. Las máquinas virtuales no lograban conectarse al servidor de pruebas la mayoría de las veces. Tenían conflictos para obtener una dirección IPv6. Algunas veces la obtenían, otras veces no. No se

encontró un patrón definido. Al hacer pruebas vía inalámbrica, los resultados fueron los mismos. Se utilizaron diferentes clientes, tanto Windows como Android. El problema se seguía presentando; los equipos con mucha frecuencia no eran capaces de obtener direcciones IPv6. No había problemas de conectividad ya que al utilizar direcciones fijas, cualquier cliente podía acceder sin problemas al servidor web de prueba.

Esta propuesta tampoco fue considerada por estas razones:

- Los resultados de las pruebas fueron en general negativos. La generación y asignación de IPs fue errática y no se podía garantizar una conexión confiable.
- Al igual que la propuesta anterior, utilizar SLAAC con el firewall supondría la alteración de la topología y/o tener equipos dedicados a dar servicio a la red IPv6.

IV.3.4 Múltiples Redes Ipv6 Con Dhcpv6 En El Access Point

Otra opción que se exploró fue la de revisar las capacidades IPv6 del Access Point. Al revisar la consola de configuración del dispositivo se encontró que este equipo tiene la capacidad de actuar como servidor DHCPv6. La Ilustración 22 muestra el menú de configuración IPv6 del equipo DIR-600.

IPv6 CONNECTION TYPE

Choose the mode to be used by the router to the IPv6 Internet.

My IPv6 Connection is : Autoconfiguration (SLAAC/DHCPv6)

IPv6 DNS SETTINGS

Obtain a DNS server address automatically or enter a specific DNS server address.

☒ Obtain a DNS server address automatically
☐ Use the following DNS address

Primary DNS Server :

Secondary DNS Server :

LAN IPv6 ADDRESS SETTINGS

Use this section to configure the internal network settings of your router. If you change the LAN IPv6 Address here, you may need to adjust your PC network settings to access the network again.

Enable DHCP-PD : ☒

LAN IPv6 Address : /64

LAN IPv6 Link-Local Address : FE80::218:E7FF:FE95:689E/64

ADDRESS AUTOCONFIGURATION SETTINGS

Use this section to setup IPv6 Autoconfiguration to assign IP addresses to the computers on your network. You can also enable DHCP-PD to delegate prefixes for router in your LAN.

Enable automatic IPv6 address assignment : ☒

Enable Automatic DHCP-PD in LAN : ☒

Autoconfiguration Type : SLAAC + Stateless DHCPv6

Router Advertisement Lifetime: (minutes)

Ilustración 22. Configuración de IPv6 en el equipo DIR-600

Para verificar su funcionalidad, se realizó una prueba sencilla en el laboratorio. Se deshabilitó temporalmente el Cisco ASA, se configuró la interface interna del DIR-600 con una dirección IPv6 y se activó la opción de servidor DHCPv6.

Los resultados fueron alentadores. Las máquinas virtuales eran capaces de adquirir una dirección IPv6 y tener comunicación entre ellas a través de ping⁴⁶. La siguiente prueba

⁴⁶ Aplicación parte de la suite de ICMP que utiliza los mensajes echo request y echo reply para probar conectividad entre equipos en la red

fue conectar equipos a la red por vía inalámbrica. Esta prueba también fue exitosa, estos equipos se podían comunicar con las máquinas virtuales utilizando IPv6.

El siguiente paso consistió en hacer una modificación al diseño del laboratorio. En esta nueva propuesta el *Access Point* funcionaría como ruteador y equipo inalámbrico al mismo tiempo. El DIR-600 se encargaría de proveer direccionamiento IPv6 a la red interna y de ser el gateway de esta red. La Ilustración 23 describe la nueva topología creada para la prueba.

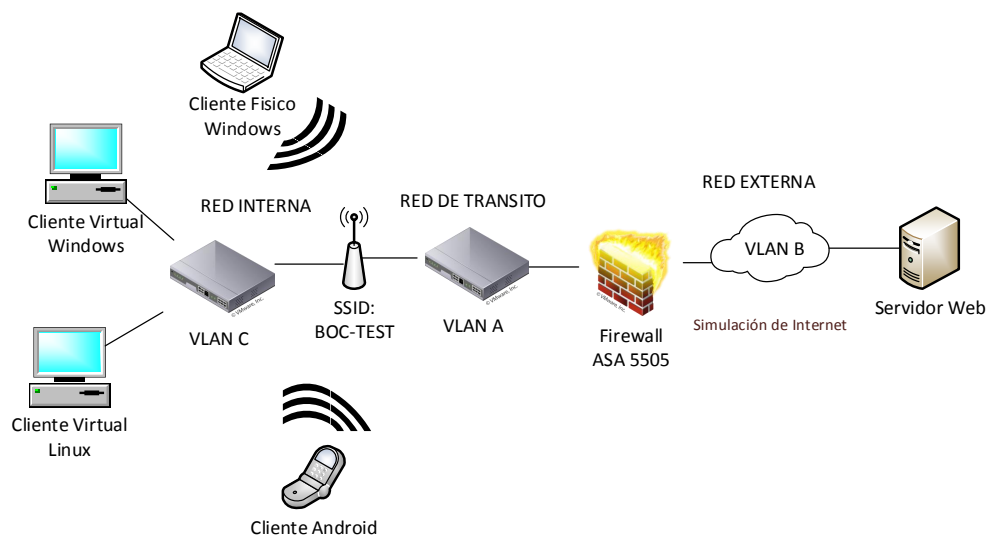


Ilustración 23. Access Point como servidor DHCPv6 y Gateway de la red

Para lograr la topología anterior, se tuvieron que realizar las siguientes modificaciones al laboratorio:

- Se creó una tercera VLAN en el switch (VLAN C)
- Se configuró el puerto de WAN del Access Point con una dirección IPv6 del segmento interno del firewall.
- Se habilitó una de las interfaces LAN del *Access Point* como *Gateway* y servidor DHCPv6 de la nueva red interna.

- Se configuró una ruta por default del *Access Point* hacia el Cisco ASA.
- En el Cisco ASA se agregó una ruta estática hacia la red interna del *Access Point*.
- Este diseño requería por lo menos dos redes, una de tránsito (VLAN C) ubicada entre el Access Point y el Firewall y la red interna (VLAN C) en la cual se encontrarían los equipos finales.

La siguiente ilustración describe los cambios de red hechos a la topología de laboratorio para probar la nueva solución.

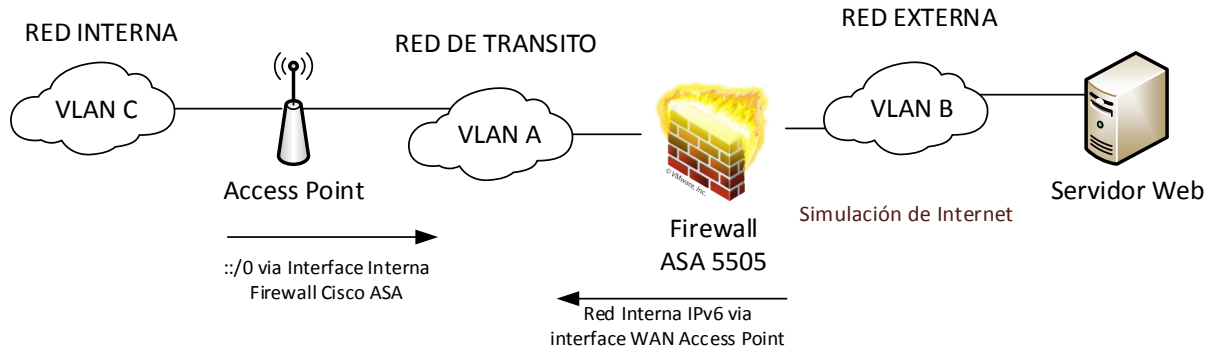


Ilustración 24. Nueva topología del laboratorio

Los dispositivos en la red eran capaces de obtener dirección IPv6 y comunicarse con otros dispositivos tanto en la red interna, la de tránsito y la externa. Se realizaron pruebas de conectividad utilizando PING ⁴⁷y TRACEROUTE⁴⁸. Desde los clientes Windows y Linux se pudo visualizar correctamente la página IPv6 en el servidor web de pruebas.

Esta fue la solución elegida por las siguientes razones:

⁴⁷ Utilería parte de la suite de ICMP con la cual se puede comprobar conectividad con un host en la red.

⁴⁸ Utilería parte de la suite de ICMP con la cual se puede determinar la ruta que tomó un paquete para llegar a su destino final

- El Access Point funcionaba correctamente como DHCPv6 para la red de clientes y los equipos conectados a ella no tenían problemas de conectividad.
- Este diseño era muy similar a la topología de IPv4 actual, lo cual no suponía cambio alguno a la topología actual.

IV.3.5 Presentación De La Propuesta De Implementación Al Cliente

A lo largo de la fase de análisis hubo constante comunicación con el cliente para estar tenerlo al tanto del avance de las soluciones que se estaban probando y los resultados de las mismas. Después de probar en el laboratorio la solución de utilizar el Access Point como servidor DHCPv6, hubo una llamada telefónica con el cliente en la cual se expuso la solución y los resultados de las pruebas. Se le planteo utilizar este diseño para la implementación ya que cumplía con todas las restricciones y funcionalidad deseada.

El cliente se sintió satisfecho con la solución y accedió a que se implementara en el laboratorio.

IV.4 FASE DE IMPLEMENTACIÓN

La siguiente sección describe las tareas ejecutadas durante esta fase, la cual culmina con la implementación exitosa de la solución antes propuesta.

IV.4.1 Documentación Del Cambio

En la sección anterior se describió como dentro del laboratorio, se configuro un ambiente con características muy similares a las del laboratorio en Rumania. Para poder ejecutar y documentar el cambio en su totalidad, dentro del laboratorio se pruebas se instaló una instancia de Cisco CSM.

El firewall de pruebas fue agregado a esta herramienta para que fuera administrado a través de ella. Una vez que esto fue realizado, se replicaron los pasos que habría que seguir. Estos pasos fueron los siguientes:

- Hacer un respaldo de la configuración actual del dispositivo
- Configurar los objetos IPv6 dentro la consola (redes y direcciones)
- Habilitar IPv6 y su direccionamiento dentro de las interfaces WAN (externa) y LAN (Interna)
- Agregar las rutas estáticas necesarias tanto para Internet como para las redes Internas.
- Configurar las reglas de acceso pertinentes.
- Aplicar los cambios al equipo a través de la herramienta

Lo anterior fue plasmado en un documento. Este documento constaba de tres secciones: Implementación, Verificación y Marcha Atrás. La sección de implementación explicaba en detalle los pasos descritos anteriormente, la de verificación contenía los pasos para verificar si el cambio había sido exitoso mientras que la de Marcha Atrás describía los pasos para regresar el equipo a su configuración original.

IV.4.2 Ventana De Mantenimiento

Esta fue una de las etapas más complicadas dentro de la fase de implementación. Dentro de INTEL no existe un mecanismo o herramienta formal para llevar control de cambios en los equipos. Por lo menos al tiempo de la implementación de este proyecto. En un principio el cliente mismo fue quien autorizo la ventana de mantenimiento, pero al no ser

el dueño del firewall en caso de haber una falla podría haber problemas con el equipo de operaciones.

El autor contactó a diversas personas para obtener un tiempo para esta implementación pero sin éxito. Se necesitó escalar esta situación con el gerente de NSE Mike M. a su vez fue quien fue contactado con Joe G. Joe fue la persona que finalmente logró encontrar al contacto adecuado para autorizar esta ventana. Esta persona fue Declan C. quien contactó a Andrei I. para preguntarle por un tiempo adecuado para la implementación, ver anexo 2. Este último accedió a realizar la ventana de mantenimiento cualquier día hábil después de las 6 pm hora local, ver anexo 3.

IV.4.3 Implementación Del Cambio

El 24 de mayo de 2014 se agendó el cambio. No fue necesario la presencia de personal del ISP ya que ellos pre-configuraron su equipo. El cambio se realizó de acuerdo al documento previamente realizado. Todas las configuraciones funcionaron de acuerdo a lo probado en el laboratorio. La implementación fue terminada en tiempo y forma sin contratiempo alguno; el autor hizo diversas pruebas para validar que funcionara correctamente. Al concluir la validación se le informó al cliente y se le pidió que realizara pruebas para corroborar que esta implementación funcionaba de acuerdo a lo esperado. La siguiente sección describe los resultados obtenidos de esta implementación.

V. RESULTADOS

Del trabajo de análisis, diseño y adecuación de la configuración del laboratorio de INTEL Rumania para soportar IPv6 e IPv4 se logró que ambos protocolos fueran soportados en el mismo ambiente. Las pruebas de conectividad desde el laboratorio hacia Internet y

viceversa se fueron exitosas. Las reglas de acceso implementadas en el firewall funcionaron acorde a lo esperado. Inclusive fue posible administrar el ruteador inalámbrico utilizando IPv6.

V.1 Verificación Interna

En esta primera etapa de verificación, se revisó que todos los dispositivos configurados para soportar *dual stack* IPv4/IPv6 tuvieran la configuración adecuada y fueran accesibles dentro del laboratorio sin problemas.

En un primer paso, se verificó que el ruteador inalámbrico tuviera las configuraciones IPv4 e IPv6 pertinentes y pudiera ser administrado desde un cliente interno a través de IPv6.

The screenshot displays the configuration interface of a wireless router. The left sidebar contains navigation links: STATISTICS, INTERNET SESSIONS, WIRELESS, IPv6, and IPv6 ROUTING. The main content area is divided into three sections: GENERAL, WAN, and WIRELESS LAN. The GENERAL section shows the system time (2000/01/01 01:05:27) and firmware version (2.16 Tue 21 May 2013). The WAN section shows a DHCP Client connection with a status of 'Connected' and a 'Renew' button. It lists the connection up time, MAC address (d8:fe:e3:77:e3:8d), IP address (192.168.1.37), subnet mask (255.255.255.0), default gateway (192.168.1.1), and DNS servers (8.8.8.8 and 4.4.4.4). The LAN section shows the LAN MAC address (d8:fe:e3:77:e3:8c), IP address (192.168.0.1), subnet mask (255.255.255.0), and DHCP server status (Enabled). The WIRELESS LAN section shows the wireless radio status (Enabled), MAC address (d8:fe:e3:77:e3:8c), 802.11 mode (Mixed 802.11n, 802.11g and 802.11b), channel width (20/40MHz), channel (9), network name (SSID) (redacted), Wi-Fi Protected Setup status (Enabled/Configured), and security (WPA/WPA2-PSK). The bottom of the page shows the 'WIRELESS' tab selected.

Section	Parameter	Value	
GENERAL	Time	2000/01/01 01:05:27	
	Firmware Version	2.16 Tue 21 May 2013	
WAN	Connection Type	DHCP Client	
	Cable Status	Connected	
	Network Status	Connected	
	Renew	Release	
	Connection Up Time	0 Day 0 Hour 56 Min 56 Sec	
	MAC Address	d8:fe:e3:77:e3:8d	
	IP Address	192.168.1.37	
	Subnet Mask	255.255.255.0	
	Default Gateway	192.168.1.1	
	Primary DNS Server	8.8.8.8	
Secondary DNS Server	4.4.4.4		
LAN	MAC Address	d8:fe:e3:77:e3:8c	
	IP Address	192.168.0.1	
	Subnet Mask	255.255.255.0	
	DHCP Server	Enabled	
WIRELESS LAN	Wireless Radio	Enabled	
	MAC Address	d8:fe:e3:77:e3:8c	
	802.11 Mode	Mixed 802.11n, 802.11g and 802.11b	
	Channel Width	20/40MHz	
	Channel	9	
	Network Name (SSID)	[Redacted]	
	Wi-Fi Protected Setup	Enabled/Configured	
	Security	WPA/WPA2-PSK	

Ilustración 25. Configuración IPv6 del Ruteador Inalámbrico

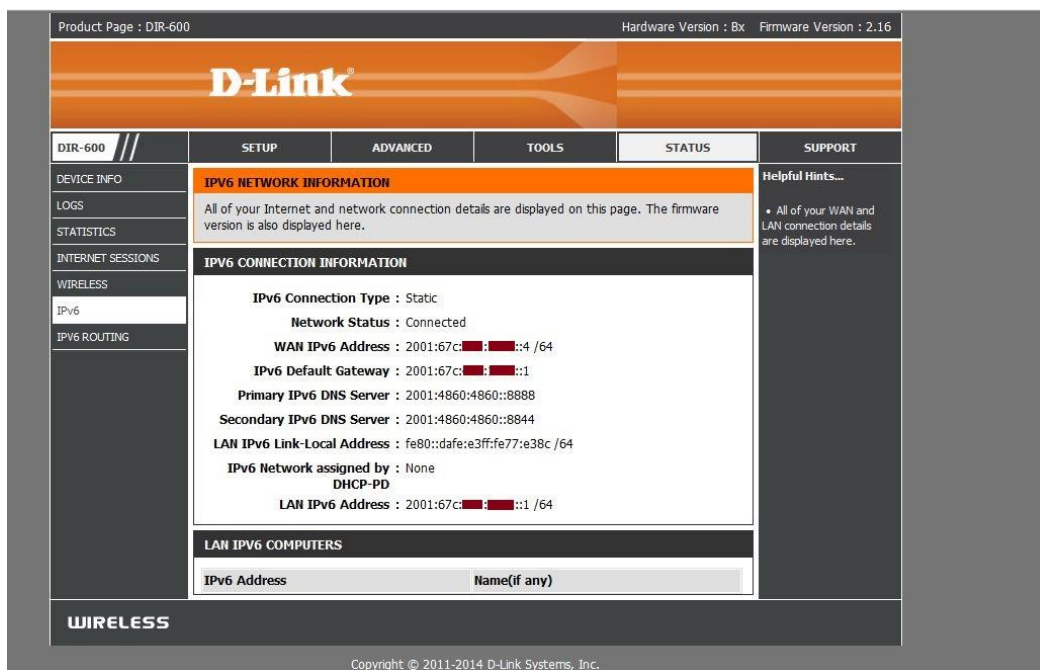


Ilustración 26. Configuración IPv6 del Ruteador Inalámbrico

El siguiente paso fue verificar que el ruteador inalámbrico tuviera conectividad IPv6 desde el ambiente interno. Esta verificación se hizo a través de la página IPv6 de administración del dispositivo. Al abrir exitosamente esta página se corroboró que IPv6 y su *stack* de TCP eran funcionales dentro del laboratorio.

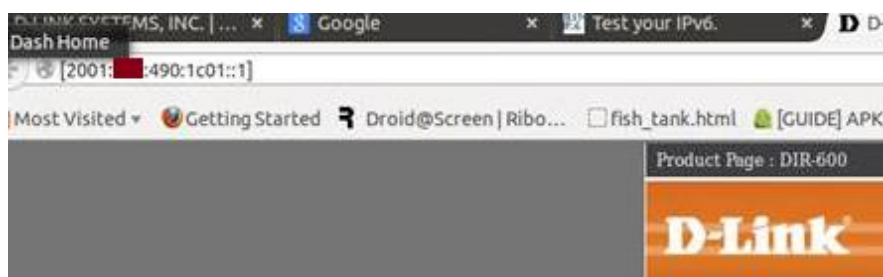


Ilustración 27. Página de Administración IPv6 del Ruteador Inalámbrico

La siguiente prueba fue verificar que el firewall, Cisco ASA, tuviera las configuraciones adecuadas y pudiera alcanzar sin problemas el equipo del ISP utilizando IPv6. Ambas pruebas fueron exitosas. Las siguientes ilustraciones muestran la configuración IPv4 e

IPv6 del firewall la cual fue hecha a través de CSM, también se muestra la tabla de ruteo IPv6 del firewall y una prueba de conectividad hacia el ISP.

Device: boc--lcfw--intel.com
Policy Assigned: -- local --

Policy: **Interfaces**
Assigned To: local device

Name	Status	Security Level	IP Address	IP Address Type	VLAN ID
inside	Enabled	100	192.168..1/255..255.0(Static) 2001::490:::1/64(Static)	static	200
outside	Enabled	0	80..150/255.255.255.248(Static) fd7d::fb::2/126(Static)	static	100

Ilustración 28. Interfaces del firewall con IPv4 e IPv6

Device: boc--lcfw--intel.com
Policy Assigned: -- local --

Policy: **IPv6 Static Route**
Assigned To: local device

Routing - IPv6 Static Route

Interface	Network	Gateway	
outside	any	boc--lcfw--c-fd7d--00fb--1	1
inside	net_2001--490---64	boc--lcfw-asus-1-2001--490-1c0...1	
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1
inside	net_2001--490---64	boc--lcfw-dir600-2-2001--490-1...1	1

Ilustración 29. Tabla de ruteo IPv6 del firewall

Device: boc--lcfw--intel.com
Policy Assigned: -- local --

Policy: **IPv6 Access Rules**
Assigned To: local device
Inherits From: -- none --

Filter: (-- none --)

No.	Permit	Source	User	Destination	Service	Interface	Dir.
1		any	-- no user --	any	NB-Group	inside	in
2		any	-- no user --	any	P2P-Drop-Group	inside	in
3		net_2001--490---60	-- no user --	any	IP	inside	in
4		any	-- no user --	net_2001-67c--60	ICMP6-Echo-Reply ICMP6-Time Exceeded ICMP6-Echo ICMP6-Packet-Too-Big ICMP6-Echo ICMP6-Packet-Too-Big	outside	in
5		net_2001--490---60	-- no user --	any		inside	in

Ilustración 30. Reglas de acceso IPv6 del firewall

```

.# ping fd7d:2973:fb::1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to fd7d:2973:fb::1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
.#

```

Ilustración 31. Conectividad IPv6 exitosa entre el laboratorio y el ISP

V.2 Verificación Externa

Una vez que se validó que el ambiente IPv6 funcionaba dentro del laboratorio, el último paso consistía en verificar la conectividad hacía internet utilizando IPv6. La primera verificación fue la de red. Se hicieron pruebas de red utilizando ping y haciendo trazas hacia servidores externos. Ambas pruebas fueron exitosas.

Test your IPv6 connectivity.

Summary
Tests Run
Share Results / Contact
For the Help De

i Your IPv4 address on the public Internet appears to be 187.247.108.224

i Your Internet Service Provider (ISP) appears to be Mega Cable, S.A. de C.V.,MX

x No IPv6 address detected [\[more info\]](#)

✓ **Good news!** Your current configuration will continue to work as web sites enable IPv6.

i You appear to be able to browse the IPv4 Internet only. You will not be able to reach IPv6-only sites.

i Your DNS server (possibly run by your ISP) appears to have no access to the IPv6 Internet, or is not configured to use it. This may in the future restrict your ability to reach IPv6-only sites. [\[more info\]](#)

Your readiness score

0/10
for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Ilustración 32. Ping desde la red interna hacia Internet

```

traceroute to ipv6.l.google.com (2a00:1450:4017:801::1009) from 2001:::490:::897f:6da3:171e
 1 2001:::490:::1 (2001:::490:::1) 0.775 ms 0.621 ms 0.612 ms
 2 fd7d:2973:fb::1 (fd7d:2973:fb::1) 7.861 ms 6.706 ms 7.58 ms
 3 2001:67c:490:1::1 (2001:67c:490:1::1) 2.164 ms 1.929 ms 5.017 ms
 4 2001:67c:490:1::a (2001:67c:490:1::a) 1.42 ms 26.369 ms 1.589 ms
 5 2001:67c:490::1 (2001:67c:490::1) 1.326 ms 1.588 ms 1.513 ms
 6 10gigabitethernet1-3.core1.buh1.he.net (2001:470:1:469::1) 1.516 ms 1.541 ms 1.49 ms
 7 10ge2-1.core1.buh1.he.net (2001:470:0:2b6::1) 12.057 ms 16.804 ms 11.996 ms
 8 google.bix.bg (2001:7f8:58::3b41:0:1) 12.06 ms 12.461 ms 13.686 ms
 9 2001:4860::4:0:84e0 (2001:4860::4:0:84e0) 12.382 ms 12.408 ms 12.214 ms
10 2001:4860:0:1::619 (2001:4860:0:1::619) 12.511 ms 12.544 ms 12.37 ms

```

Ilustración 33. Traza IPv6 desde el laboratorio hacia Internet

La tercera prueba fue verificar que se podían acceder páginas web fuera del laboratorio. La conectividad externa se verificó accediendo a la página de la red social *Facebook* para el protocolo IPv6.

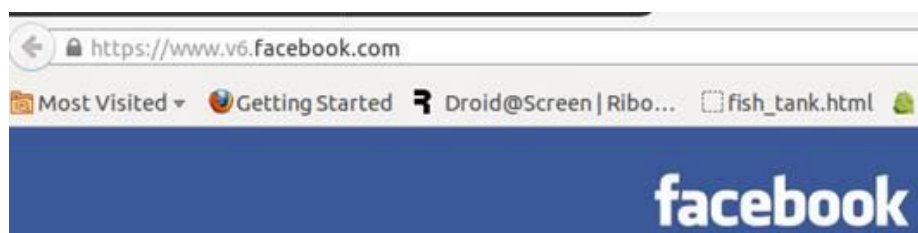


Ilustración 34. Página IPv6 de Facebook

Finalmente para validar completamente la capacidad de los clientes dentro de laboratorio para poder navegar en Internet; se utilizó el sitio web <http://test-ipv6.com/> el cual hace pruebas de conectividad y compatibilidad para clientes IPv6 e IPv4. Este sitio hace una revisión a los clientes que la consultan y determina si estos trabajan con IPv6.

Test your IPv6 connectivity.

Summary Tests Run Share Results / Contact For the Help De

Your IPv4 address on the public Internet appears to be 187.247.108.224

Your Internet Service Provider (ISP) appears to be Mega Cable, S.A. de C.V.,MX

No IPv6 address detected [\[more info\]](#)

Good news! Your current configuration will continue to work as web sites enable IPv6.

You appear to be able to browse the IPv4 Internet only. You will not be able to reach IPv6-only sites.

Your DNS server (possibly run by your ISP) appears to have no access to the IPv6 Internet, or is not configured to use it. This may in the future restrict your ability to reach IPv6-only sites. [\[more info\]](#)

Your readiness score

0/10 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Ilustración 35. Cliente sin soporte para IPv6

Test your IPv6 connectivity.

Your IPv4 address on the public Internet appears to be 80.15.150

Your IPv6 address on the public Internet appears to be 2001:490:897f:6da3:171e:5fd0

Your Internet Service Provider (ISP) appears to be IDILIS Idilis SRL,RO

Since you have IPv6, we are including a tab that shows how well you can reach other IPv6 sites. [\[more info\]](#)

Good news! Your current configuration will continue to work as web sites enable IPv6.

Your DNS server (possibly run by your ISP) appears to have IPv6 Internet access.

Your readiness score

10/10 for your IPv6 stability and readiness, when publishers are forced to go IPv6 only

Ilustración 36. Laboratorio de Rumania IPv6 funcionando

V.3 Validación Del Usuario Final

Una vez que estas pruebas fueron realizadas y documentadas se envió la comunicación indicando que la implementación ya había sido realizada. El encargado de verificar que esta implementación cumpliera con las expectativas del equipo, fue Andrei I. Este último a través de un correo confirmó que los dispositivos móviles se podían conectar correctamente a la red del laboratorio. Con este correo se dio por concluida la implementación.

VI. CONCLUSIONES

Es innegable que el protocolo IPv6 ya no es una tecnología distante. Es un hecho que IPv4 está llegando a su fin y es necesario estar preparado para la transición de un esquema de direccionamiento IPv4 a IPv6. A pesar de que este cambio va a tomar tiempo, muchas aplicaciones comenzaran poco a poco a dejar de lado IPv4 en favor de IPv6. Considero que es necesarios que todas las organizaciones comiencen a hacer pruebas y pilotos para estar preparados para esta inminente transición.

La realización de este proyecto tuvo como objetivo el habilitar el protocolo IPv6 dentro del laboratorio de INTEL en Rumania. Esta implementación se realizó con base en la experiencia previa del autor. Dado los resultados, expresados en el apartado correspondiente, podemos concluir que el proyecto fue exitoso dejando la documentación necesaria para el soporte del ambiente IPv6 del laboratorio.

De forma personal me permitió conocer más a fondo las implicaciones y los retos que una transición IPv4 a IPv6 conlleva. Así como distintos escenarios y técnicas para lograr la coexistencia de ambos protocolos en un mismo ambiente. Considero que si hubiera utilizado una metodología formal como la propuesta por la NIST los resultados hubieran sido bastante similares, pero la documentación mucho más robusta permitiendo crear un modelo para futuras implementaciones en laboratorios con características similares.

La implementación de este proyecto no solo expandió mi conocimiento técnico en el ámbito de redes, sino que también me ayudo a comprender un poco más sobre una de las líneas de negocio de INTEL a las que se le está poniendo mucho interés y como las TI fueron un elemento de suma importancia para ayudar a la organización a lograr tener en tiempo y forma la certificación de los productos y llegar al mercado en los tiempos adecuados.

Actualmente la organización de TI⁴⁹ dentro de INTEL es un centro de costos mientras que otros grupos son unidades de negocio. A pesar de que TI no genere ingresos de manera directa es un habilitador para ayudar a los demás grupos a realizar sus actividades diarias a través de la tecnología. Este proyecto es un claro ejemplo de esto.

⁴⁹ Tecnologías de Información

Sin la cooperación de TI la implementación no se hubiera realizado a tiempo, causando retrasos en la certificación y por ende no tener los productos listos para su venta en el mercado. Esto causaría pérdidas económicas a INTEL.

Termino concluyendo que para futuras implementaciones de esta naturaleza en las que sea participe buscare aplicar la metodología de la NIST para la transición de IPv4 a IPv6 con el fin de lograr mejores resultados y generar una documentación más robusta que ayude a tener un mejor control del ambiente tanto para el soporte como para la inclusión de nuevos servicios dentro del ambiente.

VII. PROPUESTA DE MEJORA

A continuación, expongo puntos de mejora que considero ayudarían a tener una mejor planeación, ejecución y documentación de este tipo de implementaciones dentro de los laboratorios de prueba de INTEL.

- **Identificar a todos los involucrados en el proyecto.** Uno de los retos principales de este proyecto fue el de identificar a todos los involucrados. A pesar de que el cliente final estaba perfectamente identificado y se tenía una comunicación constante, fue difícil encontrar a las personas encargadas de los firewalls para obtener su aprobación para realizar los cambios en el equipo y agendar una ventana de mantenimiento.
- **Analizar La Topología del Laboratorio y Evaluar Una Posible Adecuación.** La implementación pudo haber sido más rápida si se hubiera modificado la topología del laboratorio. Dentro del laboratorio se realiza un doble NAT uno en el firewall y otro en el Access Point. Esto obligó a solicitarle al ISP una red IPv6 más grande

para poder hacer el subneteo correspondiente. De igual forma fue necesario agregar más rutas dentro del firewall. En este caso no era posible hacer una adecuación al laboratorio ya que una de las restricciones era el no cambiar el sistema operativo del firewall.

- **Verificar las capacidades IPV6 de los dispositivos de red, analizar su ciclo de vida y evaluar su posible actualización.** En este caso el firewall si soportaba IPV6 pero la versión de sistema operativo que tiene no soporta ciertas características como ser servidor DHCPv6. Esto obligó a utilizar una topología de red menos eficiente. Por otro lado, el ciclo de vida de este dispositivo ya había llegado a su fin. Considero que, si antes de realizar la implementación se hubiera considerado la opción de instalar un equipo nuevo, con mejores características y un sistema operativo más actualizado, traería los siguientes beneficios:
 - **Simplificar la topología de red.** Se hubiera podido quitar el doble NAT y evitar hacer subneteo IPV6.
 - **Mejorar el desempeño de la red.** Al quitar el doble NAT se mejora la transferencia de datos en la red.
 - **Simplificar la Administración de la Red.** Solamente habría que administrar el firewall para controlar el acceso, otorgar direcciones (IPv4 e IPV6) así como evitar agregar rutas estáticas para cada red detrás de un Access Point.
 - **Hacer la red más escalable.** Al tener toda la administración en el firewall es mucho más fácil ir extendiendo la red inalámbrica sin necesidad de hacer configuraciones extra. En el modelo actual es necesario configurar

los *Access Points* para funcionar como gateways IPv4 e IPv6. De la otra forma solamente habría que configurar una IP estática para administración y la red inalámbrica.

VIII. BIBLIOGRAFÍA

- Afifi, Hossam, y Laurent Toutain. 1999. «Methods for IPv4-IPv6 Transition.» *Computers and Communications, 1999. Proceedings. IEEE International Symposium on*. Red Sea, Brittany: IEEE. 478 - 484. doi:10.1109/ISCC.1999.780953.
- AndroidHeadlines.com. 2014. *AndroidHeadlines.com*. 20 de 11. Último acceso: 17 de 11 de 2015. <http://www.androidheadlines.com/2014/11/intel-ceo-admits-intel-wont-reach-tager-70-million-mobile-chips-shipped.html>.
- ARIN. 2013. *20110203.html*. 3 de February. <https://www.arin.net/announcements/2011/20110203.html>.
- Arminen, I. 2007. «Mobile Communication Society?» *Acta Sociologica* 431-437. Último acceso: 29 de August de 2015. Mobile Communication Society?
- Baz, Arturo. 2009. *Dispositivos móviles*. Oviedo.
- Bhantnagar, Aneesh. 2015. *Gadget House*. 1 de Julio. Último acceso: 23 de Noviembre de 2015. <http://gadgetstouse.com/gadget-tech/what-is-android-safe-mode-recovery-mode-and-user-mode/36372>.
- Butler, M. 2011. «Android: Changing the Mobile Landscape.» *Pervasive Computing, IEEE* 4-7.
- Church, Karen. 2007. *Mobile Information Access: A Study of Emerging Search Behavior on the Mobile Internet*. Science Foundation Ireland, Dublin: ACM Transactions on the Web. Último acceso: 29 de 08 de 2015. doi:10.1145/1232722.1232726.
- Davies, Joseph. 2008. *Windows 2008 TCP/IP Protocols and Services*. Redmon, Washington: Microsoft Press.
- Deering, S, y R Hinden. 1998. «RFC 2460.» <https://www.rfc-editor.org>. Diciembre. Último acceso: 21 de Noviembre de 2015. <https://www.rfc-editor.org/rfc/rfc2460.txt>.
- Forbes. 2015. <http://www.forbes.com/companies/google/>. Mayo. Último acceso: 18 de Noviembre de 2015.
- Frankel, Sheila, Richard Graveman, John Pearce, y Mark Rocks. 2010. «Guidelines for the Secure Deployment of IPv6.» *National Institute of Standards and Technology Special Publication* 188.

- Gandhewar, Nisarg, y Rahila Sheikh. 2010. «Google Android: An Emerging Software Platform For Mobile Devices.» *International Journal on Computer Science and Engineering (IJCSE)* 12-17.
- Google INC. 2015. *Google Company*. Último acceso: 18 de 11 de 2015.
- Google Inc. 2015. *Compatibility Program Overview*. Último acceso: 2015. source.android.com/source/.
- . 2015. «Compatibility Test Suite (CTS).» <http://static.googleusercontent.com/media/source.android.com/en//compatibility/android-cts-manual.pdf>.
- Hall, Sharon P, y Eric Anderson. 2009. «OPERATING SYSTEMS FOR MOBILE COMPUTING.» *Consortium for Computing Sciences in Colleges* 64-71.
- IDC Research, Inc. 2015. *IDC*. August. Último acceso: 17 de 11 de 2015. <http://www.idc.com/prodserv/smartphone-os-market-share.jsp>.
- Information Sciences Institute University of Southern California. 1981. *RFC 791*. Marina del Rey, California, Septiembre. <https://tools.ietf.org/html/rfc791>.
- Jyothy, Joseph, y Kurian K Shinto. 2013. «Mobile OS – Comparative Study.» *Journal of Engineering, Computers & Applied Sciences (JEC&AS)* 10-19.
- Krajci, Iggy, y Darren Cummings. 2013. *Android on x86*. New York, NY: Apress Open.
- Kurose, James, y Keith Ross. 2012. *Computer Networking: a top down approach*. New Jersey: Pearson.
- Nordmark, E, y R Gilligan. 2005. *Request for Comments: 4213*. Octubre. <https://www.rfc-editor.org/rfc/rfc4213.txt>.
- Odom, Wendell. 2008. *CCENT/CCNA ICDN1 Official Examan Certificacion Guide*. Indianapolis: Cisco Press.
- . 2008. *CCNA ICDN2 Official Certification Guide, Second Edition*. Indianapolis: Cisco Press.
- Olifer, Natalia, y Victor Olifer. 2009. *Redes de Computadoras*. Mexico, DF: McGraw-Hill.
- Rivera, Janessa, y Rob Van der Meulen. 2015. *Gartner, Inc.* . 5 de Enero. Último acceso: 17 de Noviembre de 2015. <http://www.gartner.com/newsroom/id/2954317>.
- Smith, Brad. 2008. «ARM and Intel Battle over the Mobile Chip's Future.» *IEEEExplore* 15-18. <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4519929>.
- Tanenbaum, Andrew S. 2003. *Redes de Computadoras*. México: Pearson Education.

Teare, Diane. 2008. *Authorized Self-Study Guide: Designing for Cisco Internetwork Solutions (DESGN), Second Edition*. Indianapolis: Cisco Press.

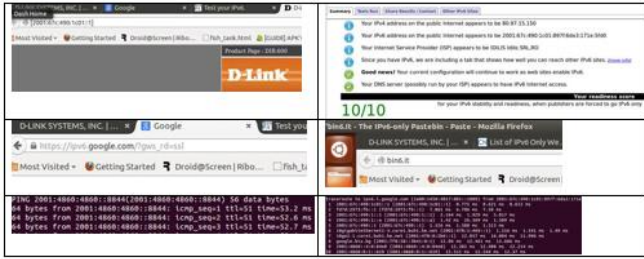
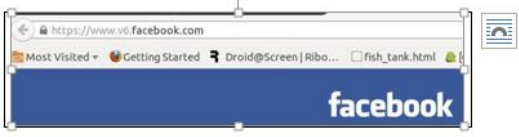
Trefis.com. 2015. *Trefis*. 21 de July. Último acceso: 29 de August de 2015. http://www.trefis.com/stock/intc/model/trefis?easyAccessToken=PROVIDER_87633ea72bd9dca1d79b8bc41462481e651ee6b5.

Vargas Beal, Xavier. 2012. *¿Cómo hacer investigación cualitativa? : una guía práctica para saber qué es la investigación en general y cómo hacerla: con énfasis en las etapas de investigación cualitativa: apropiada para quien hace investigación por primera vez*. Guadalajara: Etxeta.

Zimmermann, Hubert. 1990. «OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection.» *IEEE Transactions* 425-432.

IX. ANEXOS

IX.1 Anexo 1. Comunicación de la finalización de la implementación

<p>From: Lopez Davila, Juan Carlos Sent: Friday, October 24, 2014 12:31 AM To: Andrei, Andrei; Correa, Declan; Rene, Rene; Raul, Raul Cc: Mike, Mike Subject: RE: Downtime for CM in BOC</p> <p>Gentlemen:</p> <p>Change completed. Implementation was successful. I'm attaching some screenshots made from a local machine to verify functionality.</p>  <p>There is even an IPv6 Facebook page!</p>  <p>Andrei and I will keep working tomorrow to check access from other devices (Android)</p> <p>Thanks everybody for your help!</p> <p>--JC</p>	<p>Viernes 24 de Octubre de 2015</p> <p>Caballeros:</p> <p>El cambio ha sido completado. La implementación fue exitosa. Estoy anexado algunas imágenes tomadas de un cliente local para verificar la funcionalidad.</p> <p>Inclusive hay Facebook en IPv6.</p> <p>Andrei y yo seguiremos trabajando mañana para que otros dispositivos (Android) puedan acceder a la red.</p> <p>¡Gracias a todos por su ayuda!</p> <p>--JC</p>
Correo Original	Traducción

Anexo 1. Correo de finalización de la Implementación

IX.2 Anexo 2. Confirmación del líder de proyecto sobre la funcionalidad del laboratorio

<p>From: [REDACTED], Andrei Sent: Friday, October 24, 2014 4:50 AM To: Lopez Davila, Juan Carlos <jc.lopez@intel.com>; [REDACTED], Declan <[REDACTED]@intel.com>; [REDACTED], Rene <[REDACTED]@intel.com>; [REDACTED], RaulX <[REDACTED]@intel.com> Cc: [REDACTED], Mike <[REDACTED]@intel.com> Subject: RE: Downtime for CM in BOC Importance: High</p> <p>Hi All,</p> <p>A big thank you to all for your effort and constant support in making this happen.</p> <p>Today we made some tests on Android and it works there as well☺.</p> <p>Regards,</p> <p>[REDACTED] Andrei Romania [REDACTED] Team Lead [REDACTED] Open Source Technology Center</p>	<p>Viernes 24 de Octubre de 2015</p> <p>Saludos a todos,</p> <p>Un gran agradecimiento por su constante esfuerzo y soporte para lograr este proyecto.</p> <p>El día de hoy hicimos algunas pruebas con dispositivos Android y fueron exitosas.</p> <p>Saludos Andrei</p>
Correo Original	Traducción

Anexo 2. Correo del líder técnico validando la implementación

IX.3 Anexo 3. Buscando la autorización para la implementación del cambio

<p>From: C [REDACTED] Declan Sent: Wednesday, October 22, 2014 9:56 AM To: Lopez Davila, Juan Carlos; [REDACTED], Rene; [REDACTED], RaulX; [REDACTED], Andrei Subject: FW: Downtime for CM in BOC</p> <p>Hi Andrei,</p> <p>The infrastructure that supports your external ISP connection for labs in Bucharest needs to be reconfigured for IPv6. This will cause some downtime (JC can confirm the amount of time). Can you propose a suitable time to do this? If not you then can you let us know who should propose this time window?</p> <p>-Declan</p>	<p>Que tal Andrei</p> <p>La infraestructura que soporta la conectividad con el ISP para los laboratorios de Rumania requiere ser reconfigurada para soportar IPv6.</p> <p>Esto ocasionara una baja en el servicio (JC puede confirmar el tiempo necesario)</p> <p>¿Puedes proponer un tiempo pertinente para realizar esto?</p> <p>Si tú no eres la persona indicada para esto, ¿a quién podemos consultar?</p>
Correo Original	Traducción

IX.4 Anexo 4. Autorización del Cliente

<p>From: [REDACTED] Andrei Sent: Wednesday, October 22, 2014 10:02 AM To: [REDACTED], Declan; Lopez Davila, Juan Carlos; [REDACTED], Rene; [REDACTED] RaulX Subject: RE: Downtime for CM in BOC</p> <p>Hi Declan,</p> <p>A suitable downtime would be after 6.00 PM Romania time.</p> <p>@JC – Please do not forget to also contact the ISP so that they could sync their setup with yours.</p> <p>Regards,</p>	<p>Que tal Declan</p> <p>Un tiempo adecuado sería después de las 6 pm tiempo de Rumania.</p> <p>@JC – Por favor no olvides contactar al ISP para realizar el cambio en sincronía con ellos. Saludos</p>
Correo Original	Traducción

IX.5 Anexo 5. Ventana Agendada

<p>From: Lopez Davila, Juan Carlos Sent: Wednesday, October 22, 2014 10:16 AM To: Iorga, Andrei; Cotter, Declan; Brunnbauer, Rene; Dumitrscu, RaulX Subject: RE: Downtime for CM in BOC</p> <p>Hi Andrei/Declan</p> <p>I think 3 hours at most will be enough. I will also talk with Tibi to have someone from his side to configure IPv6 in the ISP router. Lets schedule this at 7 pm</p> <p>Thanks to everybody!</p> <p>--JC</p>	<p>Miércoles 22 de octubre de 2015</p> <p>Andrei/Declan</p> <p>Yo creo que a lo mucho 3 horas serán suficientes. También me comunicaré con Tibi para tener a alguien del lado del ISP para configurar su equipo. Hay que agendar esto a las 7 pm.</p> <p>¡Gracias a todos!</p> <p>--JC</p>
Correo Original	Traducción