UNIVERSIDAD AUTÓNOMA METROPOLITANA

DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA

Infraestructura ligera para soportar video streaming sin fisuras en ambientes móviles WLAN

idónea comunicación de resultados que presenta

Josué Vicente Cervantes Bazán

Para obtener el grado de

Maestro en Ciencias y Tecnologías de la Información

Asesor:

Dr. Luis Martín Rojas Cárdenas.

Jurado Calificador:

Presidente: Dr. Javier Gómez Castellanos.

Secretario: Dr. Miguel López Guerrero.

Vocal: Dr. Luis Martín Rojas Cárdenas.

Resumen

Las propuestas más importantes para el manejo de comunicaciones móviles no son capaces de cubrir completamente los requerimientos de comunicación de las aplicaciones a tiempo restringido de operación o *time constrained applications*, especialmente debido a la degradación del servicio que se presenta durante el proceso de handover. Esta degradación es observada por la aplicación como un bloqueo de excesiva duración y una tasa no despreciable de paquetes perdidos. Las razones de esta degradación se deben principalmente a: 1) los métodos de adquisición de direcciones a nivel de red, los cuales invierten demasiado tiempo en cumplir su tarea, 2) un intercambio de paquetes de señalización que ocurre en serie cuando éstos podrían ejecutarse en paralelo y 3) el retraso requerido para que la red establezca la nueva ruta de entrega de paquetes. Por otra parte, existen muchas propuestas para mejor el manejo del handover, entre las cuales, las propuestas llamadas proactivas han ganado gran aceptación en el medio. Si bien su importancia es reconocida, éstas presentan dos principales desventajas: su complejidad y su naturaleza invasiva. En efecto, la implantación de una solución proactiva requiere la introducción de modificaciones considerables a la infraestructura de comunicaciones móviles. En este trabajo de tesis se propone una infraestructura protocolaria de tipo cross layer que permite efectuar el proceso de handover en un tiempo compatible con aplicaciones interactivas en tiempo real. La propuesta consiste en duplicar ciertas fucionalidades de servicios relacionados con el manejo de la movilidad, tal como el protocolo DHCP, DNS y otros. Estas funcionalidades son instaladas en los access point para reducir el bloqueo del servicio y la pérdida de paquetes durante el handover.

Agradecimientos

Agradezco al Consejo Nacional de Ciencia y Tecnología, CONACYT, por el apoyo económico que me fue otorgado durante mis estudios de posgrado, a la Universidad Autónoma Metropolitana Unidad Iztapalapa, por todas las facilidades y recursos que me proporcionó durante mi formación académica.

Un agradecimiento muy especial para mi asesor el Dr. Luis Martín Rojas Cárdenas, por su paciencia, dedicación, valores y conocimiento compartido conmigo, de igual manera por las múltiples oportunidades que me dio, dado que sin él este trabajo no podría haber llegado a su fin.

Agradezco a mis padres, por su apoyo constante y sus valiosos consejos alentándome a seguir preparándome.

De manera especial, agradezco al Dr. Alfonso Prieto por la ayuda y comprensión otorgadas durante mi formación académica.

índice

1 Introducción

Desde hace unos años, los equipos móviles o MN (Mobile Node) han adquirido considerables capacidades de cómputo y comunicación, lo que hoy en día permite la implementación de novedosas aplicaciones distribuidas, tales como VoIP, IPTV/VoD, etc. Este tipo de aplicaciones, también conocidas como *Time Constrained Applications* (TCA) o aplicaciones a operación restringida en tiempo, imponen requerimientos de comunicación que sobrepasan las capacidades de servicio de algunas infraestructuras de comunicación tales como IP (Internet Protocol). En efecto, el protocolo de Internet no fue diseñado, ni para soportar comunicaciones móviles, ni aplicaciones TCA, debido a sus principios básicos de operación. En cuanto a los problemas relacionados con la movilidad, IP establece que todo equipo que opere en el seno de una red debe derivar su dirección de esta red. Bajo ese esquema, cuando un equipo se mueve de su red original a una nueva red, éste experimentará los siguientes problemas:

1) Toda comunicación se vuelve imposible debido a que su dirección IP no es válida en el nuevo contexto. En efecto, ni los equipos, ni los enruteadores que pertenecen a esta red podrán lograr una comunicación IP con el nodo visitante mientras éste tenga su antigua dirección. La adquisición de una dirección derivada de la dirección de red es la única solución.

2) Las comunicaciones en curso se pierden. Para los protocolos orientados a conexión que dependen de IP, tal como TCP, un posible reestablecimiento de la comunicación es imposible.

3) Los nodos móviles desaparecen de la red global. Normalmente, los nodos pueden ser localizados a través de un directorio local o global. Ésta es una base de datos que contiene registros que asocian el nombre de un equipo y una dirección IP. En el mundo Internet este directorio es conocido como DNS(Directory Name System). Si uno de los elementos de la asociación nombre/dirección IP cambia sin informar al directorio, el equipo no podrá ser localizado en la red. Para mantenerse en contacto en la red global , el MN debe informar al directorio cada vez que adquiere una nueva

dirección IP.

Con el fin de hacer frente a las limitaciones que presenta IP en el terreno de las comunicaciones móviles, se han propuesto diversas soluciones [2,3,4]. Aunque ellas abordan el problema desde diferentes perspectivas, coinciden en los pasos que se deben seguir para soportar la movilidad. Estos pasos pueden ser clasificados como: 1) descubrimiento de red y adquisición de dirección, 2) preservación de las comunicaciones en curso y 3) actualización del directorio global. Estos tres pasos, y los problemas que ellos abordan, serán explicados con más detalle en los siguientes párrafos.

Primeramente, cuando un MN descubre una nueva red por medio de mecanismos de bajo nivel , la fase de adquisición de direcciones comienza. El envío de un mensaje de petición de dirección hacia el AP arranca esta fase, la cual termina cuando el AP responde con un mensaje de acuse con la dirección asignada (véase en la figura 1 la etiqueta A). La segunda fase mantiene la continuidad de los procesos de comunicación en curso. Aquí la responsabilidad de mantener la continuidad del servicio recae en el MN, el cual debe anunciar al nodo correspondiente (nodo con el que el MN mantiene la comunicación, denotado como CN) todo cambio de ubicación por medio de un mensaje dedicado a este evento (véase en la figura 1 la etiqueta B). La reacción del CN es inmediatamente redirigir el flujo de datos a la nueva dirección IP (véase figura 1, etiqueta C). Estas dos fases son las más críticas debido a que durante un pequeño periodo de tiempo el MN permanece desconectado de la red. De esta manera, los paquetes de datos que llegan a su supuesto destino se pierden irremediablemente. Las fases anteriores forman parte de lo que se conoce como el proceso de handover. La tercera fase es menos crítica y se encarga de mantener la localización global del MN a pesar de sus cambios de dirección IP. La localización de un equipo en la red normalmente se logra consultando el directorio de nombres, el cual indica la posición de un equipo en términos de su dirección IP. Entonces, mantener la localización global de un MN se logra actualizando el servidor de nombres cada vez que el MN cambie de dirección IP (véase figura 1 etiqueta D).

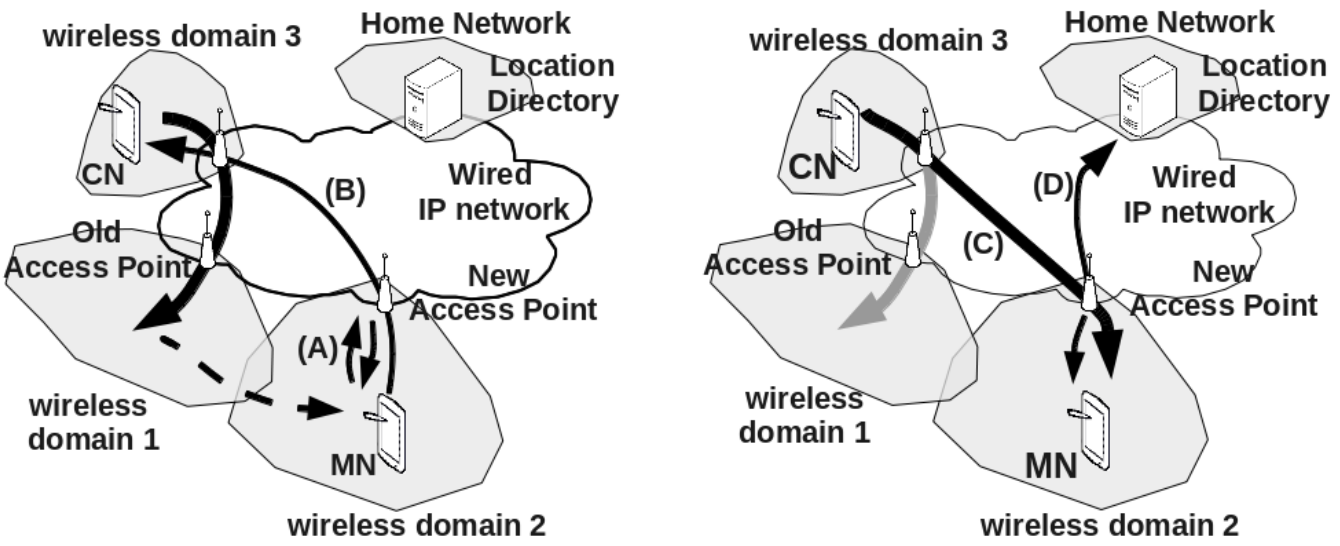


Figura 1.- Proceso de handover.

En este trabajo de tesis se propone una infraestructura protocolaria ligera que permite agilizar el proceso de handover así como reducir a cero la pérdida de paquetes. Además, nuestra propuesta es completamente compatible con los protocolos básicos para el manejo de la movilidad como IP y DHCP. Para lograr estas características, nuestra propuesta pone en juego diferentes recursos como son: la ejecución en paralelo de los procesos de señalización, la reservación de direcciones IP, el enmascaramiento del procedimiento DAD (Duplicate Address Detection), el uso de un DHCP simplificado y de la duplicación de ciertas funcionalidades de la infraestructura, las cuales se implantan directamente en los Access Points.

Dos soluciones son propuestas para agilizar el proceso de handover. Una de tipo reactiva y otro proactiva. Los dos soluciones fueron evaluadas en el marco de una aplicación de video a la demanda (VoD) implementada con Real Time Stream Protocol (RTSP) y del Real Time Protocol (RTP). El video de prueba es de tipo MPEG, integra imágenes de 720x480 píxeles y genera un tráfico de 2Mbps. Con la solución reactiva se obtiene un bloqueo de servicio de 127.3952888 ms y 26.4666918 paquetes perdidos en promedio. En cuanto a la solución proactiva, ésta ofrece un bloqueo de servicio de 115.5927044 ms pero elimina totalmente la

pérdida de paquetes. Es importante mencionar que el tiempo en el bloqueo de servicio es más o menos constante sin importar la distancia entre el cliente y el servidor gracias al uso de un mecanísmo smooth handover. En efecto, sin este mecanismo, el tiempo de bloqueo de servicio crece a medida que la latencia entre el cliente y servidor crecen. El sistema fue implementado en su totalidad bajo el sistema operativo Linux. Los nodos móviles están constituidos por Laptops dotadas con el sistema operativo Linux, mientras que los Access Points son de la marca Linksys sobre los cuales se ha instalado el firmware OpenWRT.

El resto del documento se divide en capítulos, describiendo el contexto e introducción en el capítulo I, mencionando el estado del conocimiento en el capítulo II, asimismo la infraestructura propuesta se explica en el capítulo III y en el capítulo siguiente se muestran los resultados obtenidos de la implementación, para finalmente mostrar las conclusiones en el capítulo V.

2 Estado del conocimiento

La redes inalámbricas IEEE 802.11(WLANs) juegan un rol importante para ofrecer movilidad a aplicaciones multimedia, los cuales demandan altas tasas de transferencia y mínima pérdida de paquetes para mantener una QoE (Quality of Experience) requerida por el usuario. Por otra parte la transmisión de video sobre redes inalámbricas requiere un desempeño óptimo en diferentes capas en sistemas multimedia, un paradigma cross-layer puede aplicarse para ganar un mejor desempeño en componentes individuales.

2.1 Contexto y clasificación del handover

Las nuevas generaciones de redes inalámbricas móviles, sistemas de comunicación personal, etc. han creado un nuevo método de handoff denominado handoff vertical. Dicho handoff es el proceso de cambio de red entre diferentes tecnologías inalámbricas[5] y puede clasificarse por el numero de conexiones activas que el nodo móvil mantiene durante el proceso. Es decir, al tipo de handoff que cambia de un viejo enlace a uno nuevo y además existe una corta interrupción en la transmisión después de que el viejo enlace se descarte y antes de que el nuevo enlace se haya establecido se llama “hard handoff”, este tipo de handoff solo tiene una conexión activa en cada momento. En este escenario la conexión con el objetivo es establecida antes de que la conexión con la fuente se rompa, por esta razón este handoff es llamado “Make-Before-Break”[6]. En caso contrario el “soft handoff” involucra la capa IP y enlace, durante este proceso la conexión con la fuente es rota antes de que la conexión con el objetivo se complete, por esta razón este tipo de handoff es conocido como “Break-Before-Make”[7]. Adicionalmente el handoff puede clasificarse por su desempeño en: fast,smooth y seamless.

Fast handover. Es el proceso de cambio que tiene como objetivo primario minimizar el retardo de handover, sin interés explícito en la pérdida de paquetes.

Smooth handover. Es el proceso de cambio que tiene como objetivo primario minimizar la pérdida de mensajes, sin interés explícito en los retardos por el reenvió de paquetes.

Seamless handover. Es el proceso de cambio en el que no hay cambio en la capa de

servicio, seguridad o calidad. Prácticamente se espera muy poca degradación del servicio. La definición de un handover sin fisuras prácticamente sería que otros protocolos, aplicaciones o usuarios no detectaran un cambio en la calidad, seguridad o que no detecten un cambio fuera de su funcionamiento normal. En consecuencia lo que sería un handover sin fisuras para una aplicación menos demandante, no sería igual para otra aplicación más exigente[8].

Por otra parte existen diferentes métricas para medir el desempeño de un protocolo de handoff, las principales son: el tiempo de handoff(hadoff latency), pérdidas(packet loss rate), throughput, handoff rate y signaling overload, por mencionar algunas.

Handoff-rate: es el promedio de handoffs en una llamada, para movilidad en IP se podría considerar el número de saltos que se efectúan durante una sesión multimedia.

Throughput: velocidad promedio de mensajes entregados con éxito en una red, medida en bps(bits por segundo).

Signaling overload: cantidad de señalización intercambiada entre los actores del handoff.

handoff latency: es la suma de los retardos generados en un handoff.

Packet loss rate: porcentaje de paquetes perdidos.

Todos los esquemas de cambio mencionados anteriormente soportan cambios ínter-dominio e intra-dominio, cuando un nodo móvil se cambia de red y conserva el mismo dominio de red, es decir que sólo se cambia de punto de acceso, se conoce como handoff intra-dominio, este tipo de cambio suele ser muy corto contrario al handoff ínter-dominio. Por lo tanto cuando un nodo móvil cambia de red y de dominio IP se ejecuta un handoff inter-dominio, generalmente la literatura también clasifica a las propuestas de handoff en proactivas y reactivas, una propuesta es proactiva cuando se desencadena el proceso de cambio antes de que el handoff ocurra, en cambio cuando se toman acciones después de que el nodo móvil se conecta a la nueva red es una propuesta reactiva[9].Finalmente la última clasificación del handoff que falta por mencionar es por capas, es decir en qué capa del modelo OSI, se le da solución al handoff. En medida que avance este capítulo se versará sobre algunas propuestas desde un perspectiva por capa.

2.2 Perspectiva desde la capa de enlace

En esta capa el cambio de red es conocido como “handoff-layer2” o proceso de asociación, según el estándar IEEE 802.11[10] este proceso se divide en tres etapas detección, autenticación y reasociación. En la primera etapa, el nodo móvil necesita encontrar puntos de acceso potenciales dentro de su rango, esta acción puede ser pasiva o activa[11]. En el proceso activo, el nodo móvil envía un mensaje broadcast probe request por cada canal, después activa el *probe timer* y si no recibe respuesta antes de que el temporizador alcance *MinChannelTime*, el nodo móvil considera que no hay un punto de acceso en ese canal y deberá buscar otro canal. De igual manera si el MN detecta que el canal no está oculto, debe esperar por un mensaje probe response hasta que el timer alcance el *MaxChannelTime.* Unas mediciones empíricas demuestran que el *MinChannelTime* es 20ms aproximadamente y el *MaxChannelTime* es 40ms aproximadamente[12]. Por otra parte, en el proceso pasivo, la tarjeta de red inalámbrica espera por mensajes tipo beacon, enviados periódicamente por los APs cada 100ms en cada canal. Como el estándar 802.11 tiene 14 canales; pero para Latinoamérica sólo 11 canales se usan[13], entonces tenemos un tiempo mayor a un segundo de latencia de detección lo cual es una condición no favorable para aplicaciones en tiempo real.

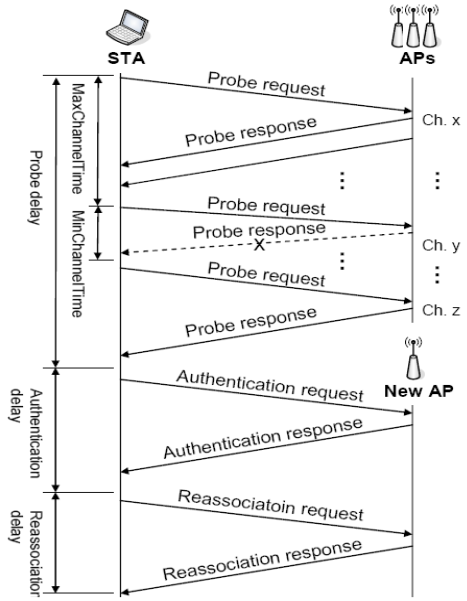


Figura 2.- Handoff layer 2[14]

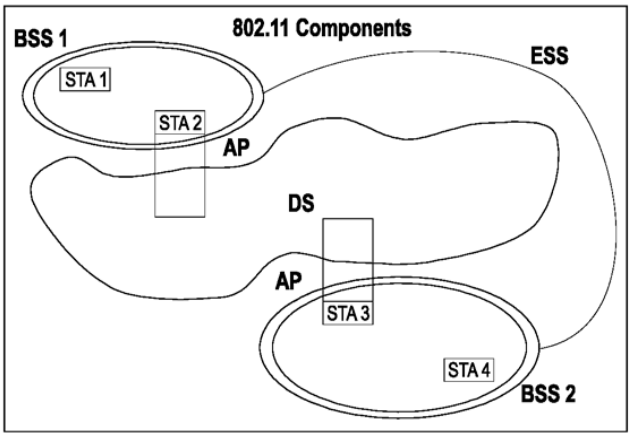
Una vez que el MN descubre los puntos de acceso potenciales, para que pueda gozar de los servicios que ofrece el AP, debe estar autenticado y asociado. A grandes rasgos, un nodo se puede autenticar o no dependiendo del esquema de seguridad, es decir, si el sistema es abierto (Open system) admite a cualquier host sin necesidad de autenticarse. En otro caso admite sólo a los MN que conocen la contraseña(Shared Key). Por otra parte el proceso de asociación consiste en el intercambio de dos mensajes entre el AP y el MN *association request* y *association response*, una vez que el nodo recibe el mensaje *association response* está listo para enviar y recibir mensajes a través del AP.

2.2.1 Adquisición de dirección

En esta capa, no se puede hablar de una adquisición de dirección, porque el protocolo de adquisición de dirección está situado en la capa de red, pero existen propuestas del tipo cross-layer para pre-arrendar las direcciones como[15,16], en las que se sobrecargan los mensajes IEEE 802.11 request para solicitar una dirección IP, al mismo tiempo que se asocian, es decir mientras se efectúa el handover layer-2.

2.2.2 Preservación de la continuidad de los servicios

El proceso de cambio de red en capa dos, en el estándar 802.11, estipula tres tipos de movilidad según el esquema que propone la Figura 3.



STA: estación móvil inalámbrica. **ESS:** extended service set, conjunto BSS
BSS: basic service set, área de cobertura de servicios básicos, donde las STA se asocian. **AP:** punto de acceso.

Figura 3.- Componentes de 802.11[17]

En el apartado 11 Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications[17], se menciona lo siguiente:

- ***No-transition:*** *en este tipo, dos subclases son identificadas , 1)static, sin movimiento, 2)Local movement, el movimiento local dentro del rango físico de la estación inalámbrica(STA) es decir , moviéndose dentro de una área de servicios básicos.*
- ***BSS-transition:*** *en este tipo de movimiento está definido como una estación inalámbrica moviéndose de un BSS(Basic Service Set) en un ESS(Extended service set) a otro BSS con el mismo ESS. Una transición rápida de BSS, establece los estados necesarios para la conexión de datos antes del proceso de reasociación preferentemente después del proceso de reasociación*
- ***ESS-transition:*** *este tipo de movimiento esta definido como una STA moviéndose de un BSS en un ESS a otro BSS en diferente ESS. Este tipo de movimiento sólo es soportado si el STA es apto para mantener las conexiones con capas superiores, el estándar 802.11 no garantiza el mantenimiento de las conexiones activas, de hecho una interrupción del servicio es probable que ocurra.*

Ninguno de los tres esquemas de movilidad anteriores, resuelve conflictos de capas superiores es por eso que protocolos como IAPP(Inter-Access Point Protocol)[18], proveen mecanismos para mejorar la transicion entre BSS. Múltiples propuestas para reducir el handoff de capa dos han surgido y muchas propuestas han llegado al consenso de que el

principal contribuyente del retardo de esta capa es el tiempo de detección, así que la mayoría de las propuestas se concentran en hacer una pre-detección, como SyncScan[19], DeuceScan[20]. El protocolo SyncScan sincroniza los AP con pequeños intervalos de tiempo reduciendo drásticamente el retraso, pero esta operación es propuesta para una detección completa de canales, en cambio DeuceScan aplica pre-detección parcial (usando gráficas de “spatiotemporal”) que es establecida a diferente tiempo y locación, pero reducir el tiempo de detección genera más tráfico de lo normal. Es por eso que [14], presenta una solución para reducir el tráfico generado por la pre-detección.

2.2.3 Manteniendo la localización global

Esta capa se centra en reducir el tiempo de detección y cuando se usan protocolos como IAPP, se habla de un protocolo que intercambia información entre APs. Por lo tanto, están en la misma red, es decir se habla de un handover inter-dominio, lo que conoce el estándar 802.11 como roaming.

2.3 Perspectiva desde la capa de red

La capa de red parece ser la preferida para manejar la movilidad IP, básicamente cuando se habla de movilidad a nivel red, se debe hablar de Mobile IP(MIP), puesto que MIP es el protocolo representativo de dicha capa. Originalmente fue propuesto por C. Perkins, *et al.*[21], en 1996, desde entonces muchos investigadores han contribuido a mejorar el protocolo.

Mobile IP define tres componentes básicos: 1)Nodo Móvil, 2)HA(Home Agent) entidad especial localizada en la red origen del nodo, el HA sabe en todo momento donde está el MN y finalmente el 3)FA(Foreign Agent), otra entidad especial localizada en la red destino, encargada de entregar los paquetes dirigidos al MN. Dichos componentes cooperan para localizar y registrar la dirección IP actual del MN que se mueve a través de diferentes subredes IP[22], es decir está diseñado para proveer un servicio de traspaso de paquetes transparente para capas superiores, comúnmente usando el protocolo *tunnelling*[23].

Dicho proceso consiste en dos fases: 1)“*agent discovery” y 2)“registration”*. Agent discovery es el periodo donde el MN detecta que se está moviendo de una subred a otra y obtiene una nueva dirección, llamada CoA(Care-Of-Address)[24]. Por otra parte el procedimiento *Registration* consiste en informar al HA la CoA del MN, con la finalidad de mantener actualizada la dirección IP del MN y reenviar los paquetes desde la red origen hasta la red destino usando un túnel virtual[25].

El grupo Mobile IP de la IETF considera siete protocolos de micro-movilidad a saber: Mobile IP Jerárquico, Fast Handoff, Proactive Handoff, TeleMIP (Telecommunications Enhanced Mobile IP Architecture), Cellular IP, HAWAII (Handoff-Aware Wireless Access Internet Infrastructure) y EMA (Edge Mobility Architecture). Los primeros cuatro protocolos son extensiones de Mobile IP, diseñados para compensar sus debilidades en micro-movilidad, y son llamados genéricamente “protocolos de gestión de movilidad basados en Agentes Foráneos (AF)”, el resto de los protocolos están basados en re-expedición de un enrutador a otro, en vez de Afs.

Cellular IP propuesto por A. Campbell et al.[78] en el año 1999. Este protocolo presenta varias ventajas 1) no utiliza encapsulamiento de paquetes, 2) es eficiente en la búsqueda de tablas de ruteo, manteniendo en primera instancia a los nodos activos, 3) establece el camino más corto entre el punto de acceso y el router de frontera(EF). Para una discusion del protocolo y sus especificaciones véase[79,80], respectivamente.

2.3.1 Adquisición de dirección

El mecanismo para la adquisición de una dirección CoA radica en los servicios del nuevo Agente FA, que periódicamente difunde un mensaje *Router Advertisement* el cual contiene información relacionada con el CoA. Este mecanismo tiene el inconveniente de que el periodo mínimo de emisión de este mensaje es de un segundo. Un mecanismo más rápido es usar el mensaje *Router Solicitation*, el cual explícitamente solicita un mensaje *Router Advertisement* considerando que el MN y el FA están en el mismo canal, esta operación toma $2t_s$ y corresponde a un tiempo de ida y vuelta(RTT) entre el MN y el FA

(véase figura 4). Por otra parte propuestas como [24, 26, 27, 28], se centran en minimizar el tiempo de handover y se pueden clasificar en dos grupos. El primer grupo tiene como objetivo minimizar el tiempo de registro usando una administración jerárquica, mientras el segundo grupo intenta reducir el tiempo de adquisición de dirección, con pre-configuraciones, generalmente se refiere a cada uno como “handoff jerárquico” y “low-latency handoff”. Aunque la combinación de ambas propuestas demuestra mejoras en el desempeño en términos de retardo que oscila entre 300 y 400 ms[29] y pérdidas de paquetes, no es suficiente para un traspaso sin fisuras.

2.3.2 Preservación de la continuidad de los servicios

Cuando la nueva CoA es adquirida, el MN debe informar al HA sobre la nueva CoA enviando un mensaje *Registration*. Después del registro, el HA ya puede reenviar los paquetes (originalmente enviados por el CN hacia la dirección origen del MN) hacia el FA por el túnel establecido y finalmente hasta la nueva CoA. Este esquema genera lo que es conocido como ruteo triangular, lo que se caracteriza por insertar un retardo adicional de extremo a extremo (end-to-end delay). Para reducir dicho retraso puede usarse una optimización de ruta o por sus siglas en ingles RO (*Route Optimization*) es decir encapsula directamente los paquetes para el actual CoA sin pasar por el HA. Este procedimiento se describe en la Figura 4.

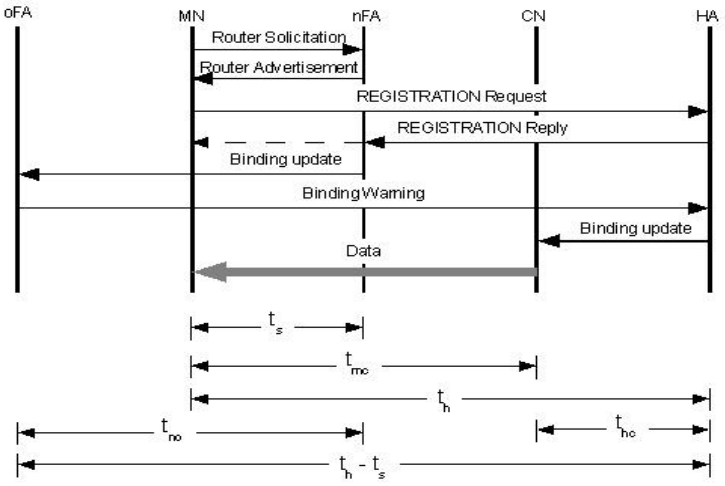


Figura 4.- Procedimiento de Handover en MIP con RO.

El HA envía al MN un mensaje Registration Reply que es interceptado por el nuevo FA (nFA) y entonces enviado al viejo FA(oFA) que a su vez envía un mensaje *Binding Warning* para el HA. Finalmente el HA envía una actualización de asociación(Binding update) para el CN que comienza a enviar los datos directamente al MN. Smooth Handoff es una funcionalidad adicional que reduce la pérdida de los paquetes durante un handover por medio de una actualización de la asociación del nFA y el oFA, de acuerdo con [25], durante el proceso de handover, el tiempo de interrupción del servicio en MIP con RO es:

$$T_{mip\_inter} = t_{no} + 3t_h + t_{hc} + t_{mc} \quad (1)$$

Donde :

t_{no} : retraso de un mensaje entre el nuevo FA y el viejo FA

t_h : es el retraso entre el MN y el HA.

t_{hc} : es el retraso entre la red origen y el CN.

t_{mc} : es el tiempo que tarda en llegar un dato desde el CN hasta el MN.

El traspaso suave(smooth handoff) comienza después del retraso de:

$$T_{mip\_smooth} = 2t_s + 2t_h + 2t_{no} \quad (2)$$

El traspaso suave previene de la pérdida de paquetes redireccionando los paquetes desde el viejo FA hacia el nuevo FA antes de que el proceso de traspaso sea completado. Un túnel creado entre los agentes foráneos ayuda en la tarea.

2.3.3 Manteniendo la localización global

No es necesario el registro en MIP para mantener la localización global porque el HA está actualizado con su nueva dirección CoA. Es decir, el agente origen conoce la ubicación de su MN en todo momento además el CN usa la dirección original para localizar al MN. Recientemente Mobile IP es ampliamente usado para soportar comunicaciones sin fisuras, sin embargo procesos innecesarios causan problemas en la escalabilidad, es por eso que es necesario investigar cómo reducir la señalización como en DLP-MIP[30], P-MIP[31,32] y TSP-MIP[33].

2.4 Perspectiva desde la capa de transporte

La capa de transporte mantiene una verdadera conexión de extremo a extremo, mientras que capas inferiores ignoran la semántica del concepto, debido a que los protocolos de movilidad se implementan en capas superiores, su unión con las aplicaciones es más fuerte, pero al introducir protocolos móviles en esta capa, la interfaz con la aplicación cambiará. Eso implica un cambio sustancial en la red, como introducción de un servidor proxy, modificaciones en el kernel del MN, etc. Sin embargo hay dos maneras de solucionarlo, la primera es recompilar todas las aplicaciones con la interfaz de transporte modificada y la otra es poner un parche en las aplicaciones de transporte, ambas soluciones son costosas y no son ampliamente desarrolladas[34]. Además las soluciones de movilidad en la capa de transporte requieren modificar las implementaciones en los nodos correspondientes a nivel transporte. Una desventaja adicional es que esto implica que usuarios estáticos deben instalar las implementaciones para comunicarse con un usuario móvil. Las soluciones para capa de transporte son muy específicas, es decir existen aplicaciones especialmente diseñadas para aplicaciones TCP o UDP, como es TCP Migrate[35]. Éste soluciona la movilidad para un solo MN a la vez, requiere de ayuda del DNS para localizar al MN y si la desconexión es demasiado larga la sesión no puede ser recuperada. Esta ha sido una solución que no ha sido ampliamente aceptada

2.5 Perspectiva desde la capa de aplicación

Manejar la movilidad en las capas de transporte y red requiere algunos cambios considerables en el kernel del MN. Ésta es la principal motivación para desarrollar soluciones en capas superiores tales como aquellas implementadas a través de servicio de comunicación en el Sesion Initiation Protocol (SIP).

SIP es capaz de soportar la movilidad de terminales, movilidad de sesiones, movilidad personal y la movilidad de servicio, además SIP ha sido ampliamente aceptado como el protocolo de señalización en las nuevas redes inalámbricas, por lo tanto SIP parece ser un candidato atractivo para la gestión de servicios comunicación en redes inalámbricas IP heterogéneas a nivel aplicación. Sin embargo, SIP implica el procesamiento en la capa de

aplicación introduciendo un considerable retraso.

2.5.1 Adquisición de dirección

Después de que el nodo móvil descubre una nueva red con procedimientos de bajo nivel, la fase de adquisición de una dirección comienza. El procedimiento comúnmente usado para adquirir una dirección IP es el protocolo DHCP(Dynamic Host Configuration Protocol). Este protocolo se basa en cuatro diferentes mensajes DHCP: DHCP *discover,* DHCP *offer,* DHCP*request,* DHCP *Acknowledge*, donde todos son mensajes UDP. El protocolo DHCP satisface la mayoría de aplicaciones que no requieren un tiempo de presentación restringido, pero parece ser inadecuado en aplicaciones de tiempo real. El principal problema está relacionado con el número de paquetes intercambiados y el tiempo que tarda el protocolo en asignar una dirección IP. Este último, es un procedimiento que evita conflictos debido a la asignación duplicada de direcciones. Dicho procedimiento se efectúa gracias al uso de mensajes ARP o ICMP, dependiendo de la implementación. Para verificar el uso de una dirección IP el servidor DHCP tiene que enviar un mensaje ICMP Echo *request* a la dirección en cuestión, antes de responder al mensaje DHCP *discover.* Si nadie responde al mensaje ICMP echo *request* en un intervalo típico de 1 a 3 segundos, entonces el servidor DHCP enviará un mensaje *offer.* En lo que al cliente se refiere, se realiza una comprobación similar.

2.5.2 Preservación de la continuidad de los servicios

El procedimiento que permite al MN preservar la continuidad de las comunicaciones en curso es conocido como *mid-call* y sigue el siguiente principio: cuando un MN alcanza a la nueva red destino, entonces una nueva dirección IP se ha adquirido y el MN envía una solicitud Re-INVITE al CN. Dicha operación se lleva a cabo sin la intervención de cualquier proxy intermediario SIP. El mensaje INVITE *request* contiene una descripción de las sesiones activas del día con la nueva dirección IP. Entonces el CN inicia el envío de datos a la nueva ubicación del MN tan pronto como recibe el mensaje Re-INVITE.

De acuerdo con [25], el retardo total del traspaso con el protocolo SIP, debe considerarse la resolución de direcciones ARP en el protocolo DHCP, el retardo de la

actualización del LD o Home Register(HR), el tiempo que tarda en llegar el mensaje re-INVITE desde el MN hacia el CN y el tiempo en que tarda en llegar el primer dato desde el CN hacia la nueva locación del MN.

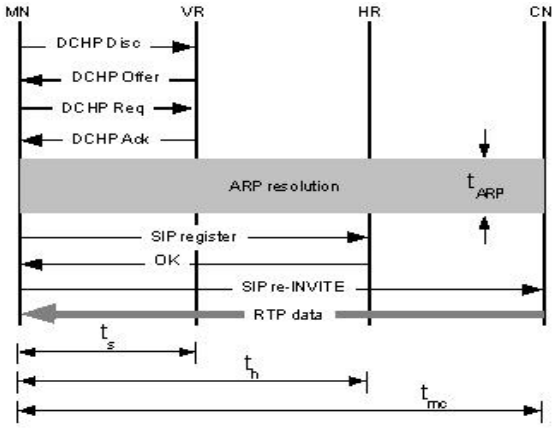


Figura 5.- Proceso de handover en SIP

Es decir el tiempo total de traspaso está dado por la siguiente expresión:

$$T_{sip\_inter} = 4t_s + t_{arp} + 2t_h + 2t_{mc}. \quad (3)$$

Donde:

$4t_s$: Corresponde a los cuatro mensajes intercambiados por DHCP

t_{arp}: Corresponde al tiempo que tarda el proceso DAD(Duplicate Address Detection) en resolver si una dirección está ocupada

$2t_h$: Es el tiempo de actualización del HR.

$2t_{mc}$: Corresponde al tiempo que tarda en llegar el mensaje INVITE desde el MN hacia el CN y el tiempo en que tarda en llegar el primer dato desde el CN hacia la nueva locación del MN.

Un inconveniente de esta propuesta es la pérdida de paquetes durante el proceso de handover, lo que también puede ser visto como un periodo de interrupción, mientras MIP soluciona esa problemática implementando un smooth handoff, SIP carece de dicho mecanismo, en consecuencia todos los paquetes transmitidos durante $2t_s + 2t_h + 2t_{no}$ se perderán.

2.5.3 Manteniendo la localización global

El procedimiento de localización global se logra mediante el envío de un mensaje de actualización al HR, que actualiza la ubicación del MN que permite a los futuros clientes alcanzar al MN con la misma URL

2.6 Problemáticas de adquisición de direcciones

Cuando un host llega a una nueva red, debe configurarse de acuerdo al contexto de red al que llegó, es decir adquirir una dirección IP, DNS, gateway, etc. Esta configuración se hacía con el protocolo Bootstrap[36], después llegó el protocolo DHCP (Dynamic Host Configuration Protocol[37] que actualmente es uno de los protocolos más aceptados para asignar direcciones IP, pero este protocolo tarda de 1-3segundos [38] para asignar una dirección IP, debido al Duplicate Address Detection(DAD), principal causante del excesivo retardo. El DAD es la entidad responsable para prevenir que diferentes clientes tengan la misma dirección IP y se ejecuta cada vez que un cliente solicita una dirección IP.

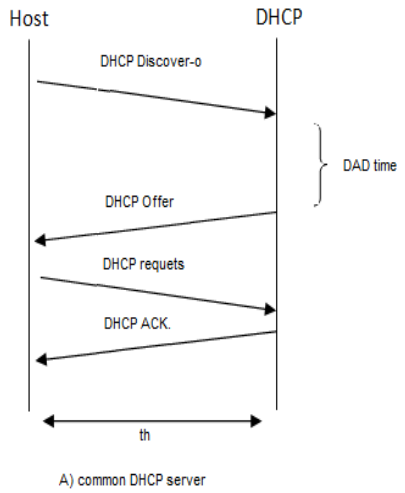


Figura 6.- Proceso para obtener una Dirección IP con el protocolo DHCP.

La mayoría de las propuestas están de acuerdo en minimizar el tempo que tarda el DAD en decidir si una dirección IP está ocupada, como en [39] que proponen una función pasiva detector de direcciones duplicadas(PDAD), ellos proponen un firmware que informa al servidor DHCP la asociación de la dirección IP con la dirección MAC, de esta forma el DAD

no se ejecutará cada que alguien solicite una dirección IP, logrando reducir la negociación de una dirección IP en cuatro mensajes, pero la recolección de información de direcciones IP, es computacionalmente costoso. Por otra parte en [40], proponen insertar la dirección IP, en los mensajes de asociación, para reducir el exceso de señalización y delegar la responsabilidad de solicitar una dirección IP al access point, pero su propuesta no elimina el tiempo de DAD y sólo reduce tiempo cuando se cambia físicamente de access point y está dentro del dominio es decir un handover intra-dominio. De igual manera en [41], proponen un protocolo Cross-layer para pre-arrendar la dirección a un MN, su propuesta consiste en agregar información a el mensaje 802.11 Probe Request, para que el AP ejecute a nombre del host la negociación con el servidor DHCP, para que cuando se asocie y autentique su dirección IP esté lista. Esta propuesta logra reducir el tiempo un 18 % (300ms), propuestas recientes como[42] está ubicada en el contexto de reconfiguración rápida basada en DHCP para redes 802.11x, pero ellos presentan una manera diferente a pre-arrendar la dirección, proponen ejecutar simultáneamente los procesos en un cambio de red, en consecuencia su retardo no puede ser bajo dado que la ejecución de DHCP no se reduce. La literatura presenta múltiples maneras de reducir el tiempo de adquisición de una dirección IP, minimizando el tiempo del DAD, pero pocas propuestas se preocupan por la seguridad o el exceso de tráfico generado. En el capítulo IV se presentará una nueva manera de obtener una dirección IP, sin introducir exceso de señalización, logrando negociar una dirección IP con sólo dos mensajes en un tiempo de ida y vuelta.

2.7 Problemáticas sobre mecanismos suavizadores de pérdidas

En el proceso de conmutación de red habrá pérdidas de paquetes si no se cuenta con un sistema que recupere y reenvíe los datos a la nueva red mientras el MN se configura. Para redes WLAN utilizando mecanismos compatibles con SIP el tiempo de bloqueo(t_{unable}) está dado por la suma del tiempo de asociación(t_a) más el tiempo de configuración de dirección IP(t_{IP}), y el tiempo que tarda en informar al nodo correspondiente su nueva dirección(t_{CN}).

$$t_{unable} = t_a + t_{IP} + t_{CN} \qquad (4)$$

Donde:

t_{unable} : Tiempo de bloqueo en redes 802.11x.

t_a : Tiempo que tarda un nodo móvil en asociarse a un AP según la tecnología 802.11a/b/g/n.

t_{IP} : Tiempo que tarda el mecanismo en asignar una dirección IP, usualmente por DHCP 1-3s.

t_{CN} : Tiempo que tarda al MN en informar al CN que ha cambiado de red, dos veces el retardo de extremo a extremo entre el MN y el CN, este tiempo está en función de la distancia a la que se encuentre el servidor.

De la ecuación anterior podemos deducir que entre más lejos esté el nodo correspondiente, mayor será el tiempo de bloqueo, por lo tanto mayores pérdidas. Los retrasos de extremo a extremo que puede haber entre el MN y CN, para un ámbito nacional pueden ser de 32-78ms[73], en cambio para comunicaciones continentales excede los 150ms[73]. Esto genera una variabilidad en el retardo y es necesario tomar acciones para mitigar la pérdida de paquetes originado por el retraso, por eso es imprescindible un proceso que suavice las pérdidas.

El principal mecanismo del reenvió de paquetes es “IP in IP tunneling”[42], en esencia el tunneling encapsula un paquete dentro de otro paquete, para poder transportarlo sobre la red. La principal ventaja del tunneling radica en montar protocolos no soportados por la red, es decir, se envuelve un paquete en otro y de esa manera puede ser transportado por la red, pero es necesario empacar y desempacar los paquetes. De esta manera se genera una sobrecarga(overhead).

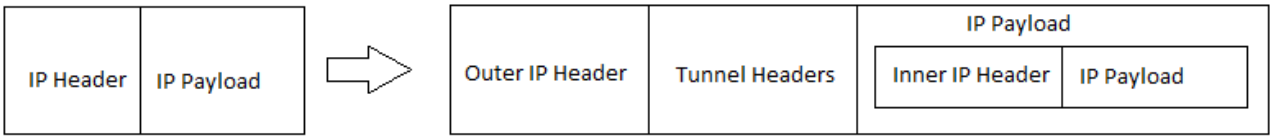


Figura 7.- Imagen ilustrativa del protocolo IP to IP tunnelling.

Mobile IP utiliza al protocolo tunneling como mecanismo para suavizar la pérdida de paquetes. En este contexto los paquetes son enviados a su Home Agent y el HA empaqueta

los datos para reenviarlos al Foreign Agent, entonces el FA desempaqueta los mensajes para ser entregados al MN. Durante este proceso, el overhead se incrementa. Es por eso que en la literatura hay abundantes propuestas para reducir la sobrecarga generada por el tunneling, enfocándose en comprimir los encabezados para reducir el overhead como [42,43,44,45,46]. Por eso, es necesaria una propuesta que no introduzca sobrecarga y no necesite una entidad que encapsule o desencapsule paquetes. Más adelante en le capítulo IV se detallarán dos propuestas con tales características, MSHO-P(Mecanismo suavizador de pérdidas proactivo) y MSHO-R(Mecanismo suavizador de pérdidas reactivo).

2.8 Problemáticas en ambientes móviles en streaming de video sin fisuras

Muchas propuestas se han desarrollado intentando solucionar el problema del traspaso de red, algunas propuestas se enfocan en dar solución por capas(enlace,transporte, red, aplicación, etc). Otras, intentar dar solución en las fases de traspaso(detección de redes, obtención de dirección IP, etc).Por otro lado, algunas propuestas implementan protocolos cross-layer, pero todas tiene como objetivo principal generar un traspaso de red con muy pocas pérdidas en el menor tiempo posible. Según el ITU-T, los tiempos de handover para un flujo de datos de video, son:

- menos de 50ms-recomendado.
- 50-150ms aceptable.
- 150-400ms condicionalmente aceptable.
- mayor a 400 inaceptable.

Aunque la tolerancia a la interrupción de servicio está en función del tipo de datos, siempre será necesario reducir más el número de pérdidas y tiempo de handover. Por otra parte la mayoría de los trabajos se centran en MIP, y múltiples propuestas han surgido tal como FMIP, HMIP, entre otras. Ahora las nuevas propuestas son para IPv6, de igual manera múltiples artículos se están enfocando a redes WMNs(Wireless mesh networks), donde hay varios tópicos de investigación, como son protocolos de ruteo rápidos, handoff en redes

mesh. Considero que reducir las pérdida de paquetes y tiempo siempre será imperativo, comparando algunas propuestas de la bibliografía se creó una tabla(véase, Tabla 1) de algunas propuesta revisadas que son aptas para transmitir video en redes WLAN.

Nombre del artículo	No.	Año	Layer	Proactiva Reactiva	Protocolo base	Tipo de handoff fast smooth seamless	Handoff rate	Losse rate	Bit rate	Handoff latency	PSNR
A Seamless Handoff Mechanism for DHCP-Based IEEE 802.11 WLANs	[58]	2007	layer-2	reactiva	802.11 WLAN	seamless	-	-	.	< 50ms	-
Cross Layer Fast Handoff for SIP	[59]	2007	layer-7	proactiva	SIP, DHCP	seamless	-	4%	62.5 kbps	< 100ms	-
Collaborative Handover Mechanism for Real-Time Services	[60]	2009	cross-layer	proactiva reactiva	MIH, FMIP	seamless	-	-	64 kbps	< 50ms	-
Multimedia Ready Handoff Technique for 802.11 Networks	[61]	2007	layer-2	proactiva	802.11 WLAN	fast	-	4%	75 kbps	< 16ms	-
On Supporting Handoff Management for Multi-Source Video Streaming in Mobile Communication Systems	[62]	2008	layer-3	proactiva	FMIP	fast	-	5%	19.4 kbps	< 110ms	-
Performance Analysis of Streamed Video Over Mobile IP Based Networks	[63]	2011	layer-3	proactiva	MIP	fast	6	-	-	< 326ms	-
Pre-allocation of DHCP leases: a cross-layer approach	[64]	2011	cross-layer	proactiva	DHCP	fast	10	-	-	< 300ms	-
Video Session Handoff between WLANs	[65]	2010	cross-layer	proactiva	DHCP IAPP	fast	-	20%	-	-	15 db
Video Stream Splitting and Merging using Dual Mobile-IP Tunnels in Wireless Handoffs	[66]	2010	layer-2	proactiva	MIP	fast	-	10%	-	-	-
A Lightweight Algorithm for Fast IEEE 802.11 Handover	[67]	2012	layer-2	proactiva	802.11 WLAN	fast	-	1%	-	< 43ms	-
Handover Evaluation for	[68]	2012	layer-3	reactiva	MIP	fast	-	40%	2387	<2000	-

Mobile Video Streaming in Heterogeneous Wireless Networks									kbps	ms	
Location Base Fast MAC handoffs in 802.11	[69]	2008	layer-2	proactiva	802.11 WLAN	seamless	-	-	-	<100 ms	-
Access network controlled fast handoff for streaming multimedia in WLAN	[70]	2007	layer-2	proactiva	802.11 WLAN	seamless	-	-	-	< 29 ms	-
A pre-registered Handoff scheme in IEEE 802.11r Wireless Local Area Networks	[71]	2010	layer-2	proactiva	802.11r WLAN	fast	-	-	-	-	-
A Framework for Fast Handoff in IEEE 802.11 Based Systems	[72]	2009	layer-2	proactiva	802.11 WLAN	fast	-	-	64 kbps	<200 ms	-
Design, Implementation, and Evaluation of Cellular IP	[78]	2000	layer-3	reacrtiva	802.11 WLAN	hard y semisoft	50	1%	5 kbps	80ms	-

Tabla 1.- Tabla comparativa de diferentes protocolos de handoff.

2.9 Aspectos de seguridad

El “spoofing” o suplantación de identidad es uno de los ataques más comunes en la red para negar el servicio de acuerdo a sus siglas en inlgles DoS (Denial of Service), de acuerdo a [47], hay al menos cuatro mil ataques de ese tipo cada semana en Internet. Este tipo de ataque es muy efectivo para negar el servicio, además este tipo de ataque otorga dos ventajas al hacker. Primera, debilita la posibilidad de mitigar el ataque ya que el tráfico malicioso no puede ser clasificado por fuente y hace más difícil filtrarlo. Segunda, hace más difícil encontrar la fuente que está generando el tráfico malicioso.

2.9.1 ARP spoofing

La técnica de spoofing consiste en emitir varios paquetes ARP reply, con el fin de actualizar las tablas ARP de los equipos en la red y una dirección IP se asocie a otra interfaz, suplantando la identidad de un host, logrando obtener el flujo de datos emitido hacia el host original. Además, existen diversos ataques de suplantación de identidad, que puede ser

desde DHCP, DNS, WEB, etc. En la bibliografía existen varias propuestas para mitigar los ataques, los diferentes trabajos van desde: poner filtros en la red, hasta etiquetar los paquetes que envían por la red,etc[48]. Recientemente D. Bruschi *et al* propone un protocolo llamado S-ARP(secure ARP)[49], el cual previene la inyección de paquetes espurios en la red, utilizando un par de llaves, una pública y otra privada.

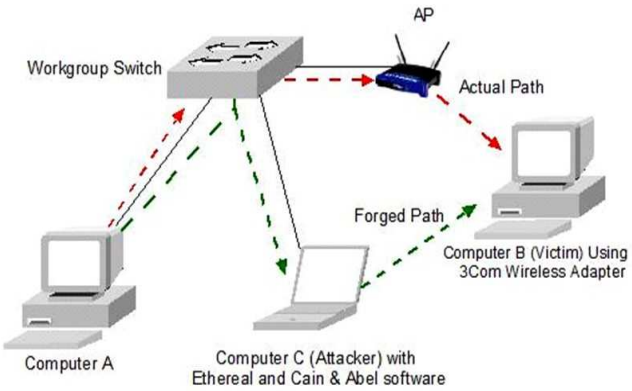


Figura 8.- ARP spoofing[50].

2.9.2 DHCP spoofing

DHCP spoofing, consiste en replicar los mensajes DHCP *request* más rápido que el servidor DHCP legitimo, con la finalidad de enviar configuraciones falsas, tales como: puerta de enlace, servidor DNS,etc. Forzando todo el tráfico a pasar a través de la máquina controladora, permitiendo capturar o modificar datos importantes. Este tipo de intrusión puede detectarse buscando múltiples respuestas para un mensaje DHCP *request* originarias de múltiples máquinas. Como se mencionó anteriormente también hay diferentes ataques documentados de suplantación de identidad a servidores DNS, WEB, etc. Por otra parte el WEB spoofing consiste en suplantar la identidad de un servidor web, este tipo de ataques tienen como objetivo enviar configuraciones falsas a los clientes, para lograr dirigir el flujo a servidores falsos y analizar las tramas del cliente.

2.9.3 DoS: Negación del Servicio

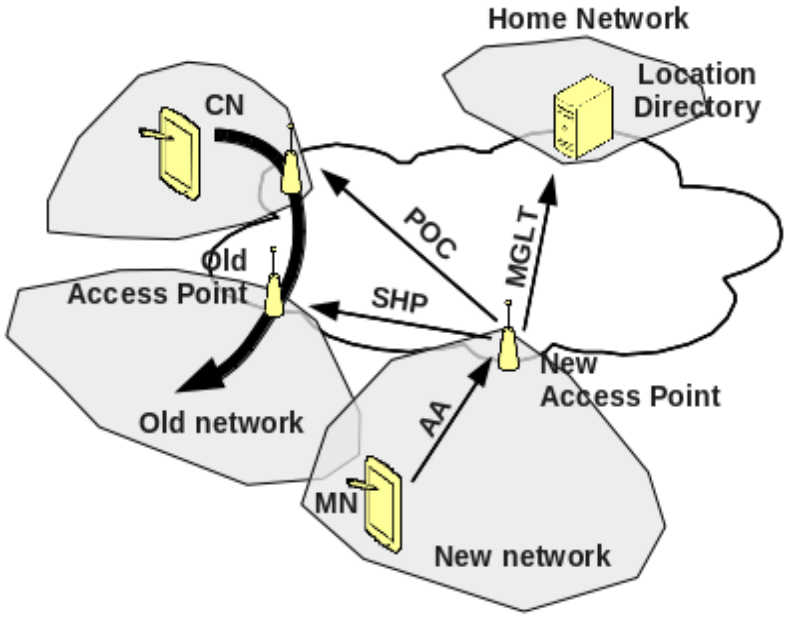
La negación de servicio consiste en no aceptar la solicitud del cliente debido a saturación en el servidor. Por otra parte, no asignar una dirección IP debido a un malware es igualmente negación de servicio. Afortunadamente este caso es ampliamente estudiado por la

literatura[51,52], y propuestas como Komori and Saito en [53] y [54] proponen usar certificados de autenticación, mejorando la seguridad, sin necesidad de pasos adicionales excepto por un pequeño overhead en los paquetes. La característica de los certificados parece una solución fácil de implementar y segura.

3 FCLH: Fast Cross-Layer Handoff

En este capítulo se describirá la propuesta llamada Fast Cross-Layer Handoff (FCLH), que es capaz de mejorar el desempeño de la comunicación móvil con respecto a las propuestas descritas anteriormente en un contexto de servidores de audio/video fijos y clientes móviles.

La propuesta FCLH está basada en la idea de ejecutar en paralelo los tres procedimientos principales que son necesarios para soportar comunicaciones móviles, 1)adquisición de dirección, 2)preservación de las comunicaciones y 3)localización global, dichas acciones se pueden iniciar por un solo mensaje. El procesamiento paralelo es posible porque se basa en tres entidades diferentes: el Nodo Correspondiente (CN), el directorio de ubicación (LD) y los dos Access Points (AP) involucrados en el proceso de traspaso. Siendo más específicos, el CN está involucrado en la preservación de la continuidad de los servicios (POC), el LD ayuda a mantener al nodo móvil alcanzable desde cualquier lugar (MGLT) y los APs son los responsables de asignar una dirección (AA) y soportar un traspaso suave (SHP). En principio como estas tareas no son del todo dependientes, se pueden efectuar en paralelo. El mensaje que desencadena todos los procedimientos es el paquete DHCP *Discover*, pero el mensaje debe ir sobrecargado con información relativa a los procedimientos que se inician. Por ejemplo, si el CN se pone en contacto por medio del protocolo SIP, el mensaje DHCP *Discovery* debe incluir el mensaje re-INVITE que apoya el comienzo del procedimiento de POC. Se propone introducir esta información en las opciones de DHCP, dado que la carga útil del mensaje DHCP depende de la unidad máxima de transmisión (MTU) de la red visitada y los mensajes SIP que participan en este estudio son pequeños, es decir un mensaje re-INVITE usa 140 bytes aproximadamente de longitud, por lo tanto, un mensaje DHCP/WiFi puede trasmitir varios mensajes, la siguiente figura representa el mecanismo del protocolo FCLH y la interacción entre las diferentes entidades.



AA: asignación de direcciones
POC: Preservación de la continuidad de los servicios
UGLT: Actualización global de localización
SHP: Proceso smooth handover

Figura 9.- Mensajes emitidos por el servidor FCLH al recibir un mensaje DHCP *discover-o*.

3.1 Adquisición de direcciones

En términos generales la propuesta entrega una dirección IP en sólo dos mensajes, esto es posible porque el FDHCP negoció varias direcciones IP con un servidor DHCP común, para lograr dicho propósito es necesario tener un servidor DHCP original y el FDHCP estará ejecutándose en el router. Básicamente el servidor FDHCP será un intermediario entre el servidor DHCP común y el cliente móvil, de hecho el servidor FDHCP únicamente va a responder mensajes DHCP *discover* con la opción 215[57] habilitada(DHCP *discover-o*) que soliciten una dirección IP rápida.

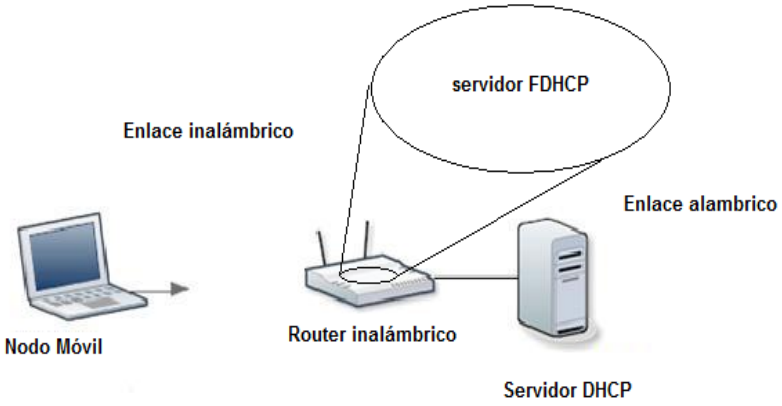


Figura 10.- Arquitectura FDHCP

Cuando un nodo móvil quiere obtener una dirección IP rápida, envía un mensaje DHCP *discover-o,* inmediatamente el servidor FDHCP envía un mensaje DHCP ACK, por otra parte el servidor DHCP común responde con un mensaje DHCP Offer, pero el tiempo de respuesta es más grande que el del servidor FDHCP, entonces el cliente ignorará la respuesta del servidor DHCP, tal como se muestra en la Figura 11, de esta manera es posible negociar la dirección con sólo dos mensajes y ambos servidores pueden coexistir entre sí.

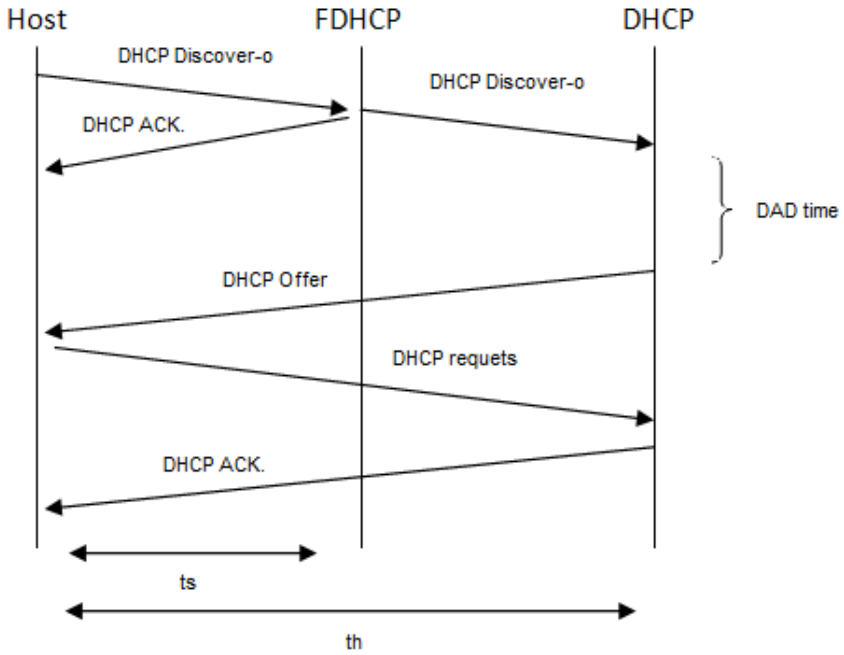


Figura 11.- Negociación de una dirección IP con la propuesta FDHCP .

Sea t_s el tiempo que tarda el mensaje DHCP *discover-o* en llegar al servidor FDHCP y sea t_h el tiempo que toma en llegar el mensaje DHCP *discover-o* al servidor DHCP común, entonces consideraremos a t_{FDHCP} como el tiempo que tarda en asignar una dirección IP el servidor FDHCP; de igual manera sea t_{DHCP} el tiempo que toma el servidor DHCP común en asignar una dirección IP, tomando en cuenta la topología de red t_{FDHCP} es menor que t_{DHCP}, por lo tanto el cliente siempre recibirá primero el mensaje DHCP ACK del servidor FDHCP.

Tiempo total en obtener una dirección IP.

$$t_{FDHCP} = 2t_s \quad (5)$$

$$t_{DHCP} = 4(t_h) + t_{DAD} \quad (6)$$

Donde:

t_s : es el tiempo que tarda en llegar un mensaje del host al servidor FDHCP.

t_h : es el tiempo que tarda a un mensaje en llegar al servidor DHCP server, aproximadamente $2t_s$.

t_{DAD} : Es el tiempo que tarda el mecanismo de detección de duplicidad de direcciones en completarse.

Por otra parte consideremos el caso en que el servidor no pueda asignar una dirección IP, tal como se muestra en la Figura 12, dicha falla no afecta la negociación de la dirección IP, porque el cliente continuará con la negociación de la dirección IP con el servidor DHCP común debido a la atención exclusiva de mensajes DHCP Discover-o genera la ventaja de tolerar fallas.

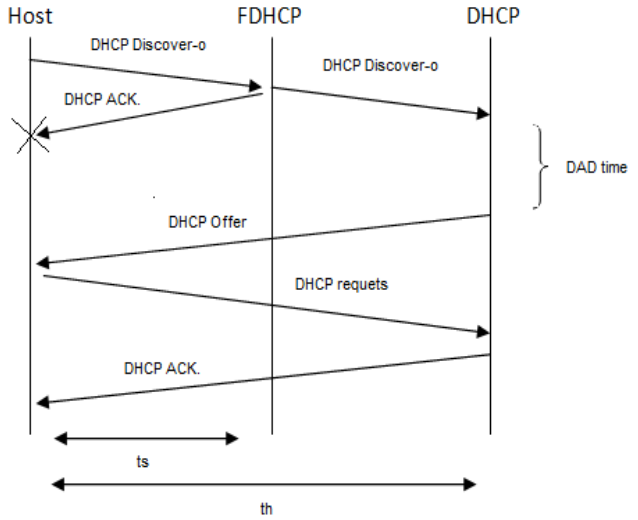


Figura 12.- Pérdida de un mensaje DHCP ACK del FDHCP.

Finalmente se obtiene un protocolo tolerante a fallas, que puede asignar una dirección IP en un tiempo de ida y vuelta, sin modificar la funcionalidad del servidor DHCP común. Además la arquitectura propuesta reduce el tráfico de mensajes porque el número de mensajes intercambiados para la obtención de una dirección es sólo dos, de igual manera el servidor FDHCP funciona sin interferir con el servidor DHCP común y es más rápido que el servidor DHCP común, por otra parte el servidor FDHCP es una pieza clave para el manejo de la movilidad, porque con este sistema se reduce el retardo del handover.

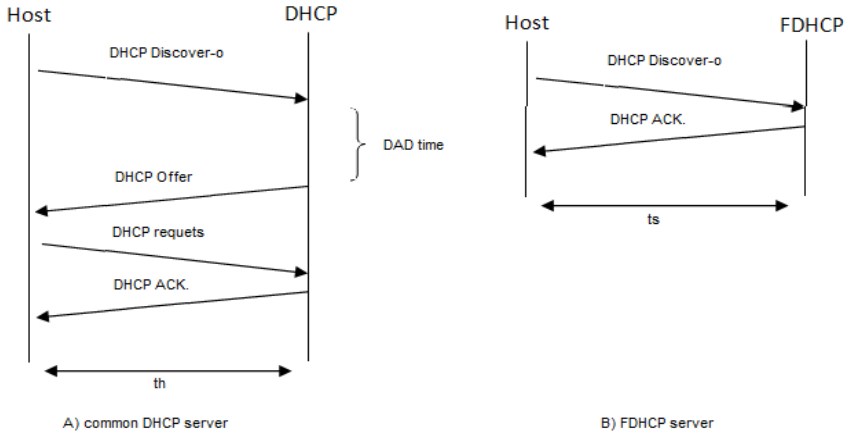


Figura 13.- A) Intercambio de mensajes para la negociación de una dirección IP con el protocolo DHCP. B) Intercambio de mensajes para la negociación de una dirección IP con el protocolo FDHCP

3.2 Preservación de la continuidad de los servicios

En el mismo instante en que el AP envía el mensaje DHCP ACK hacia el MN, el AP en otro hilo de ejecución envía el mensaje SIP Re-invite para el CN. En efecto el punto de acceso construye un mensaje SIP usando la información contenida en las opciones del mensaje DHCP *Discover*. Para poder enviar dicho mensaje, el AP actúa como router y emula el mensaje SIP re-INVITE , como si lo hubiera mandado el MN. Esto es posible porque el AP decide qué dirección IP asignará al MN de la lista de direcciones reservadas. Una vez que el mensaje re-INVITE ha sido aceptado por el CN, éste finalmente envía un OK de respuesta al MN.

Los diferentes procesos de handover son descritos en la Figura 14. Hay que hacer notar que el enfoque es Cross-Layer porque un mensaje genera otro mensaje SIP re-INVITE sin respetar la secuencia clásica de los eventos ni la jerarquía de las capas del protocolo.

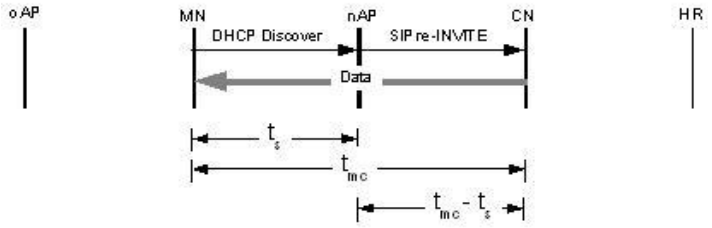


Figura 14.- Preservando al continuidad de los servicios en el proceso de handover.

EL proceso de bloqueo en un handover con FCLH es como sigue:

$$T_{fclh\_inter} = t_s + (t_{mc} - t_s) + t_{mc}$$

$$T_{fclh\_inter} = 2t_{mc} \qquad (7)$$

Un traspaso suave con el protocolo FCLH se obtiene mediante el reenvío de flujo de datos recibidos por el viejo AP (oAP) y enviados por el CN al viejo AP antes de que el CN supiera que el MN cambio su punto de conexión de red. El nuevo Access Point solicita este servicio al oAP enviando un mensaje que contiene la vieja y nueva dirección. En contraste

con MIP, la propuesta no requiere establecer un túnel ni la encapsulación de los datos originales en un flujo de datos. Esto mejora el desempeño y simplifica la implementación.

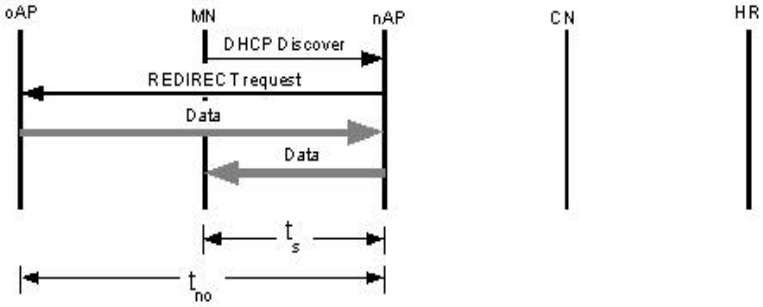


Figura 15.- Traspaso suave en FCLH.

Más específicamente, el punto de acceso tiene que cambiar únicamente los encabezados IP de los paquetes, recalculando el CRC (Cyclic Redundancy Check), y finalmente reenviando el flujo de datos para la nueva dirección, véase la Figura 15. El tiempo requerido para lograr un traspaso suave es calculado como sigue:

$$T_{fclh\_smooth} = t_s + t_{no} + (t_{no} + t_s)$$

$$T_{fclh\_smooth} = 2t_s + 2t_{no} \qquad (8)$$

3.3 Manteniendo la localización global

Una vez más, el mensaje SIP register es generado por el nAP después de la recepción del mensaje DHCP *discover-o.* Tanto, la información contenida en el mensaje como la dirección IP elegida por el nAP son usadas para generar el paquete SIP *Register.* El MGLT(mantenimiento de la localización global) es descrito en la Figura 16.

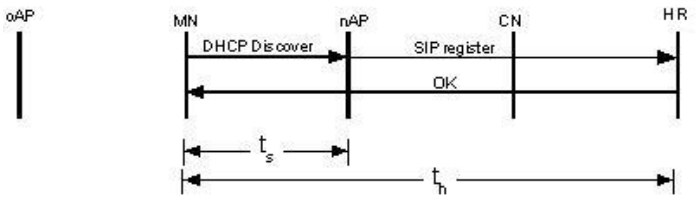


Figura 16.- Manteniendo la localización global.

El retardo requerido para actualizar el LD, o el HR en este contexto de SIP, es únicamente t_h.

3.4 Desempeño Analítico

Esta sección está basada en el análisis anterior. Más precisamente se compara el desempeño de la propuesta con MIP y SIP, con un flujo de datos de voz IP(VoIP). Por lo tanto las condiciones de prueba son las mismas a las usadas aquí. Se asume t_s = 10 ms que corresponde a un canal con un ancho de banda relativamente bajo. Para la red cableada que conecta a los AP, se considera un mayor ancho de banda, por lo tanto un menor retardo, entonces t_{no} = 5 ms. Por otra parte, se considera que el tiempo de procesamiento de las otras entidades en insignificante y menor a 1ms.

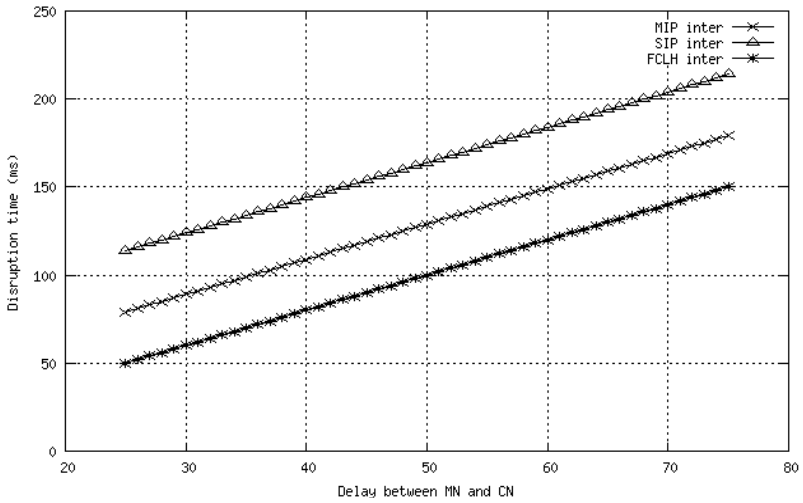


Figura 17.- Tiempo de interrupción vs el retardo entre el MN y el CN.

Se consideran tres configuraciones. En la primera, el MN está conectado a la red vía inalámbrica y la distancia del CN varía. En la segunda configuración, el CN y el MN están cerca; pero lejos de la red origen del MN. Finalmente, en la tercera configuración el retardo del canal inalámbrico varía.

A través de las ecuaciones 7 y 8 se obtuvieron los datos que se presentan en la Figura 17. Se puede observar que el tiempo de interrupción se incrementa cuando aumenta el retardo entre el MN y CN (t_{mc})

En la Figura 18, t_h se incrementa y tanto el MN como el CN son cercanos, entonces t_{mc} = 25 ms. Asimismo, el retardo del enlace es igual a 10 ms. Observe que el tiempo de bloqueo asociado a SIP se vuelve más pequeño que MIP, cuando el retardo entre el MN y la red origen(HN) es mayor a 30ms, debido al incremento del retardo entre el MN y su red origen. Entonces, el tiempo de bloqueo de MIP aumenta debido a que el retardo de traspaso depende de los registros con el HR. Por otra parte, en cuanto a nuestro enfoque se refiere, el tiempo se mantiene constante porque el tiempo de bloqueo no está en función del retardo de extremo a extremo entre el CN y el HN.

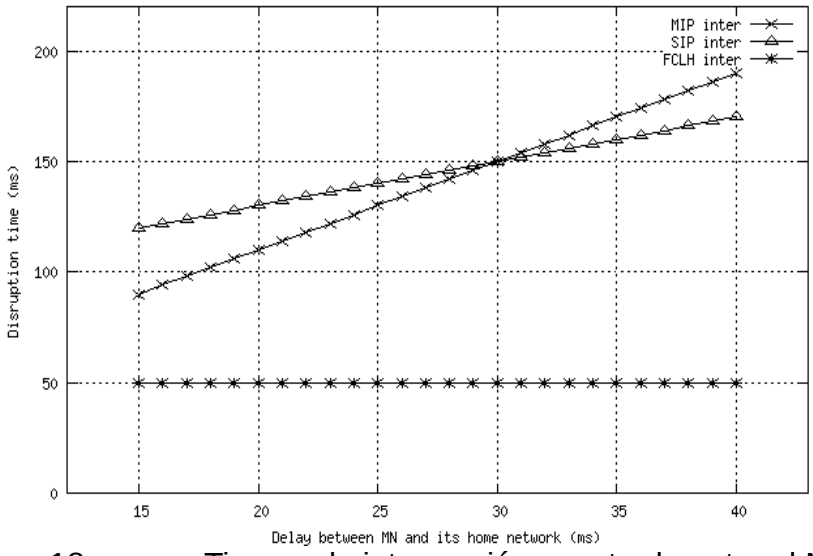


Figura 18.- Tiempo de interrupción vs retardo entre el MN y HN.

Finalmente, el último escenario demuestra el impacto del retardo inalámbrico sobre el tiempo de bloqueo, véase Figura 19. Se puede observar que el impacto de este parámetro es limitado en el caso de la propuesta FCLH. Este resultado es debido a la minimización de la señalización de cambio de paquete sobre el canal inalámbrico durante el traspaso.

En cuanto a la transferencia suave se refiere, MIP toma ventaja sobre SIP que carece de dicho mecanismo. Cayendo en cuenta que el tiempo de MIP con traspaso suave $t_{mip\_smooth}=2t_s+2t_h+2t_{no}$, además que el MN en MIP inicia la recepción de datos antes de que el

traspaso se complete. Este periodo puede calcularse como sigue, $T_{mip\_inter} - T_{mip\_smooth} = T_{mip\_inte} -$ 54 ms véase Figura 20. En la propuesta $T_{fclh\_handoff} = 2t_s + 2t_{no}$, además el nodo móvil recibe los paquetes por un periodo de tiempo igual a $T_{fclh\_inter} - T_{fclh\_handoff} = T_{fclh\_inter} - 30$ ms véase Figura 13. El periodo de traspaso suave comienza antes que MIP, es decir, la propuesta puede recuperar paquetes lo más pronto posible y por más tiempo antes que el traspaso se complete. De hecho, el traspaso suave debe comenzar tan pronto como sea posible con el fin de no degradar la percepción del usuario durante un traspaso.

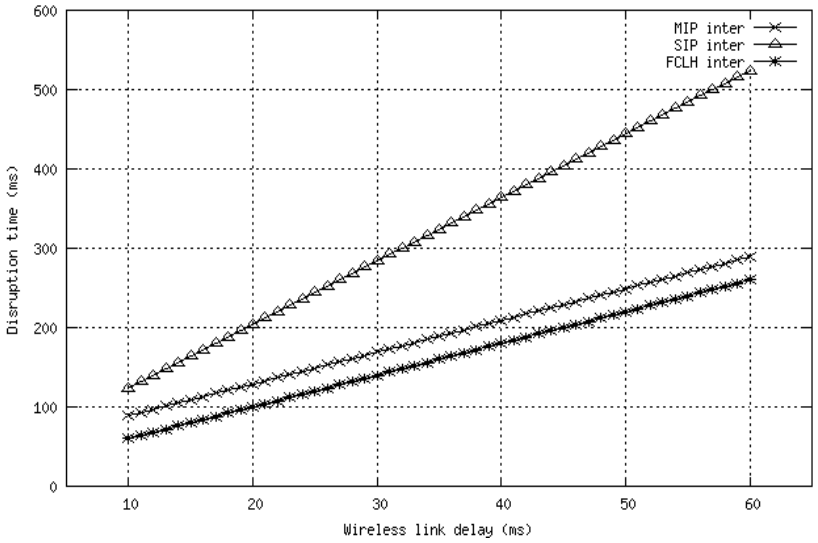


Figura 19.- Tiempo de bloqueo vs retardo del enlace inalámbrico

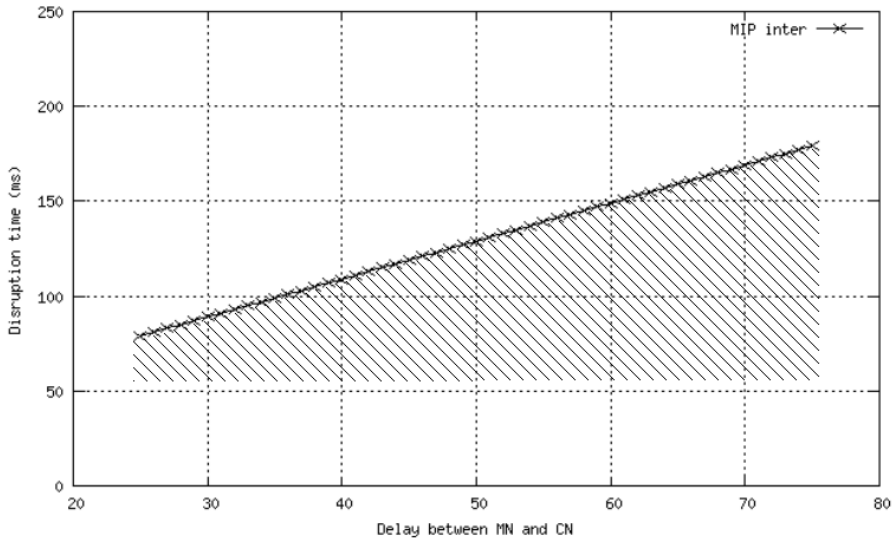


Figura 20.- Smooth handoff para MIP.

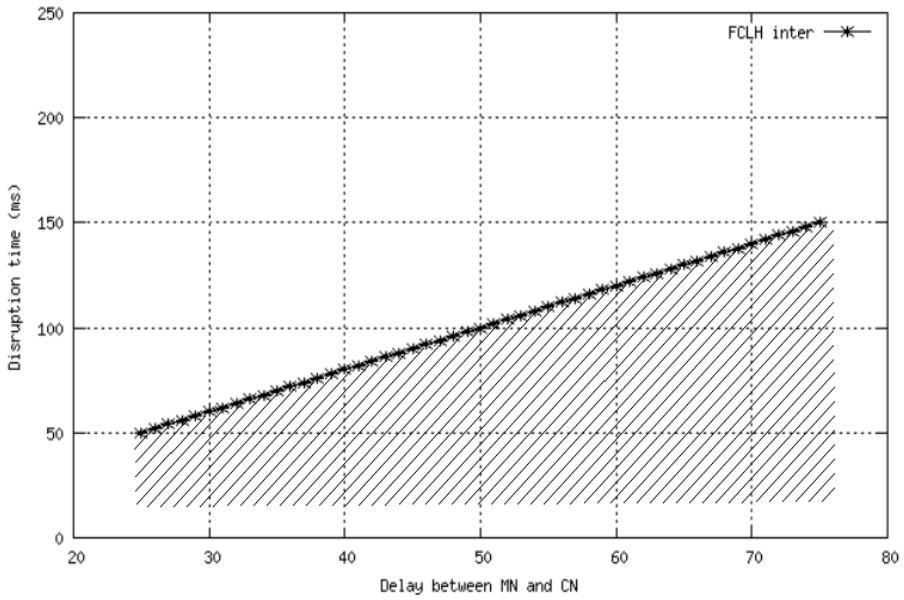


Figura 21.- Smooth handoff para FCLH.

4 Implementación y resultados

El protocolo FCLH, está diseñado para atacar a los principales problemas que atañen al handover, primordialmente el lento proceso de adquisición de una dirección IP y la pérdida inherente de paquetes. Es por eso que se muestran a continuación los principales aportes del protocolo, así como su implementación y resultados. Además la propuesta se programó en lenguaje C, con uso de sockets RAW y threads, debido a que el protocolo FDHCP debía ser ejecutado en el punto de acceso, recurrimos a routers Linksys®, con firmware openWRT[55], versión de Linux 2.6.32.25, 16MB en RAM y velocidad de CPU a 200MHz; como el AP es un sistema como capacidad de 4MB de memoria ROM no es posible cargar un compilador, es por eso que se utilizó un cross-compiler, llamado BUILDROOT[76], para construir el programa. Para poder ejecutar la propuesta en el acces point, se copió el archivo ejecutable al directorio "/bin" y se modificó el script de arranque para que el FHCP se ejecutara al encenderse. Según la arquitectura propuesta necesitamos un servidor DHCP común externo, es por eso que instalamos un servidor DHCP[56] en una PC, con sistema operativo Linux , versión de kernel 2.6.28-19, procesador Centrino core duo a 1.6 GHz y 1 GB de RAM. Por otra parte para medir el tiempo que tarda en asignarse una dirección, se usó la librería "time.h", solicitando 100 direcciones para cada uno de los niveles con los que se recibe la señal, de igual manera usando algunas herramientas del propio OpenWRT, logramos monitorear el tráfico generado, la memoria usada y las conexiones activas.

4.1 FDHCP: Fast Dynamic Host Configuration Protocol

En este capítulo se explicará la implementación de la propuesta y se evaluará su desempeño. Después de que el MN llega a una nueva red la fase de adquisición de una dirección comienza. En el contexto de la propuesta FCHL, se utiliza el protocolo FDHCP propuesto anteriormente. Éste propone reducir, de cuatro a dos, el número de mensajes necesarios para adquirir una dirección IP por el servidor DHCP. Asimismo, contribuye a eliminar el retraso generado por el DAD(Duplicate Address Detection). Para lograrlo se implementó un sistema de reserva de direcciones. Bajo este esquema, un proceso que se ejecuta en el punto de acceso reserva un número de direcciones IP y desde el punto de vista

del DAD las direcciones IP parecen no estar disponibles. Además, la propuesta es completamente compatible con un MN. Es decir, aun sin la propuesta puede operar directamente con el protocolo DHCP clásico, porque el MN puede distinguir entre un contexto FCLH y uno clásico por las opciones incluidas en el paquete DHCP ACK. En cuanto el MN se da cuenta de que el paquete DHCP ACK no incluye las opciones que esperaba, entonces comienza el procedimiento clásico. Por otra parte, cuando un servidor DHCP clásico recibe un mensaje DHCP *Discover* con opciones sobrecargadas, solamente eliminará las opciones que no conoce y continuará con el procedimiento clásico, la Figura 8 muestra el proceso en FCLH.

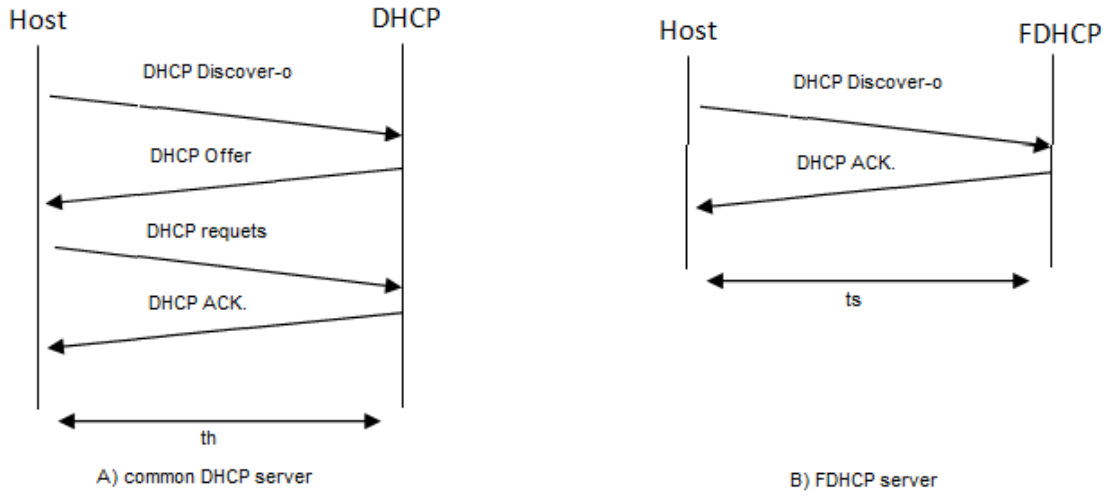


Figura 22.-A. Intercambio de mensajes para la negociación de una dirección IP con el protocolo DHCP.
B. Intercambio de mensajes para la negociación de una dirección IP con el protocolo FCLH.

Bajo el esquema anterior una dirección IP puede ser asignada desde el nuevo Access Point(nAP), en sólo $2t_s$, donde t_s, es el retardo del canal entre el MN y el AP.

4.1.1 Servidor FDHCP

El servidor FDHCP está constituido por tres módulos, el primer módulo llamado “get IPs”, es la entidad que se encarga de solicitar “n” direcciones IP al servidor DHCP común, realizando el intercambio de los cuatro mensajes y esperando el tiempo necesario para la asignación de una dirección IP, es decir espera el tiempo del DAD. El segundo módulo es

llamado “hold address”, esta entidad se encarga de responder los mensajes ARP *request* enviados por el DAD, este módulo es importante porque de esta manera se asegura que la dirección IP asignada por el FDHCP es única. Finalmente el tercer módulo llamando “FDHCP server” es responsable de atender la solicitud de una dirección IP únicamente a mensajes DHCP Discover-o.

Figura 23.- FDHCP módulos y orden de ejecución

La Figura 23 muestra los módulos y el orden de ejecución, el primer módulo en ejecutarse es “get IPs”, una vez lleno el stock de direcciones está listo para poder otorgar direcciones, entonces se ejecutan paralelamente los dos módulos restantes, uno para atender a los clientes y otro para prevenir la reasignación de las direcciones IP reservadas dinámicamente.

4.1.2 Cliente FDHCP

El cliente FDHCP se encarga de solicitar una dirección IP rápida y configurar la tarjeta de red. Este proceso es el encargado de recopilar (gathering) la información necesaria antes de realizar un handover. Es decir, obtiene la dirección IP actual, así como las direcciones IP de los servicios activos, para poder insertarlas como opciones dentro de un paquete sobrecargado DHCP *discover-o.*

La información necesaria que se solicitará e insertará es la siguiente:

- Opción 224 **Fast IP Address**: Nueva opción para identificar la petición de una dirección IP rápida. También, podría usarse la opción 80 “rapid commit option”.
- Opción 225 **Old IP address**: Dirección IP que tenía el nodo móvil en el AP viejo.

- Opción 226 **Ongoing Comunication**: Las direcciones IP de los servidores, con los que el MN tenía un servicio activo.

Al formato de paquete DHCP *discover* se le agregará la información antes mencionada dentro de las opciones libres , cada opción insertada en el paquete DHCP debe respetar su formato según el RFC 2134 se estipula que las opciones deben tener el siguiente formato:

Código	Tamaño	Información					
ccc	t	i	i	i	i	i	i

Figura 24.- Formato de opciones en paquetes DHCP.

Código: Identificador de la opción, tamaño un byte.
Tamaño: Tamaño de la información almacenada en la opción, tamaño un byte.
Información: Información adicional insertada en un campo opción, tamaño múltiplos de un byte.

Siguiendo el formato de las opciones listamos las tres opciones insertadas en el paquete DHCP *discover-o*.

Opción 224: **Fast IP address**, esta opción sirve para obtener una dirección IP rápida desde un servidor FDHCP.

Código	Tamaño	Información			
224	4	F	A	S	T

Figura 25.- Formato de opción 224: Fast IP address.

Opción 225: **Old IP address**, esta opción sirve para manejar la movilidad e informar al nuevo AP la dirección IP que tenía en el viejo AP.

Código	Tamaño	Información			
225	4	a1	a2	a3	a4

Figura 26.- Formato de opción 225: Old IP address.

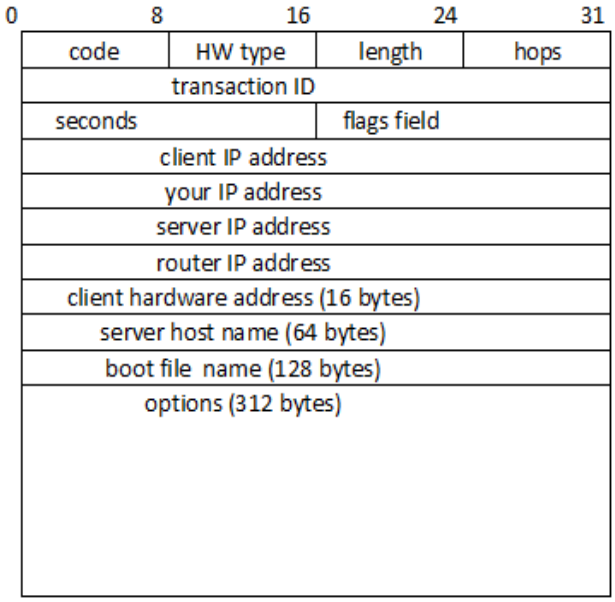
Opción 226: **Ongoing comunication**, esta opción mantiene activas las comunicaciones en curso que se tenían en el viejo AP. La longitud mínima de las opciones es cuatro octetos y el tamaño debe ser un múltiplo de cuatro octetos.

Código	Tamaño	Información						
226	n	a1	a2	a3	a4	a1	a2	.....

Figura 27.- Formato de opción Ongoing Comunication.

Finalmente reunida la información necesaria e insertada apropiadamente en el paquete DHCP *discover-o* obtendremos un paquete sobrecargado con tres opciones como muestra la Figura 28.

A)



B)

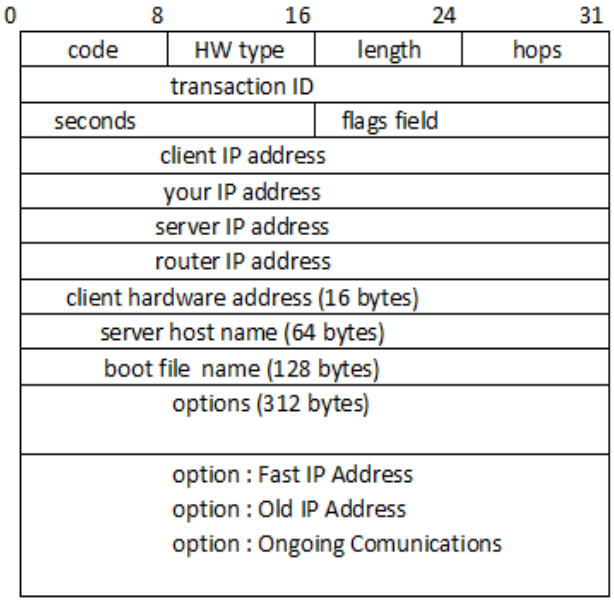


Figura 28.- Figura A Formato de mensaje DHCP original Figura B Formato de Mensaje DHCP para protocolo FCLH.

Finalmente el intercambio de dos paquetes para adquirir una dirección IP, entonces el MN envía el mensaje DHCP *discover-o* en broadcast, esperando como respuesta del servidor FDHCP un paquete DHCP *ack* con la dirección IP asignada. Acto seguido el host procede a configurar la tarjeta de red. Al finalizar este proceso se obtiene una dirección IP en un RTT y el sistema queda configurado de tal manera que es compatible con el nuevo entorno de red y a partir de ese momento el MN está listo para enviar y recibir mensajes.

4.1.4 Evaluación del desempeño

Las medidas de desempeño a considerar en esta propuesta son: el tiempo de adquisición de una dirección, cantidad de memoria usada y porcentaje de procesador usado.

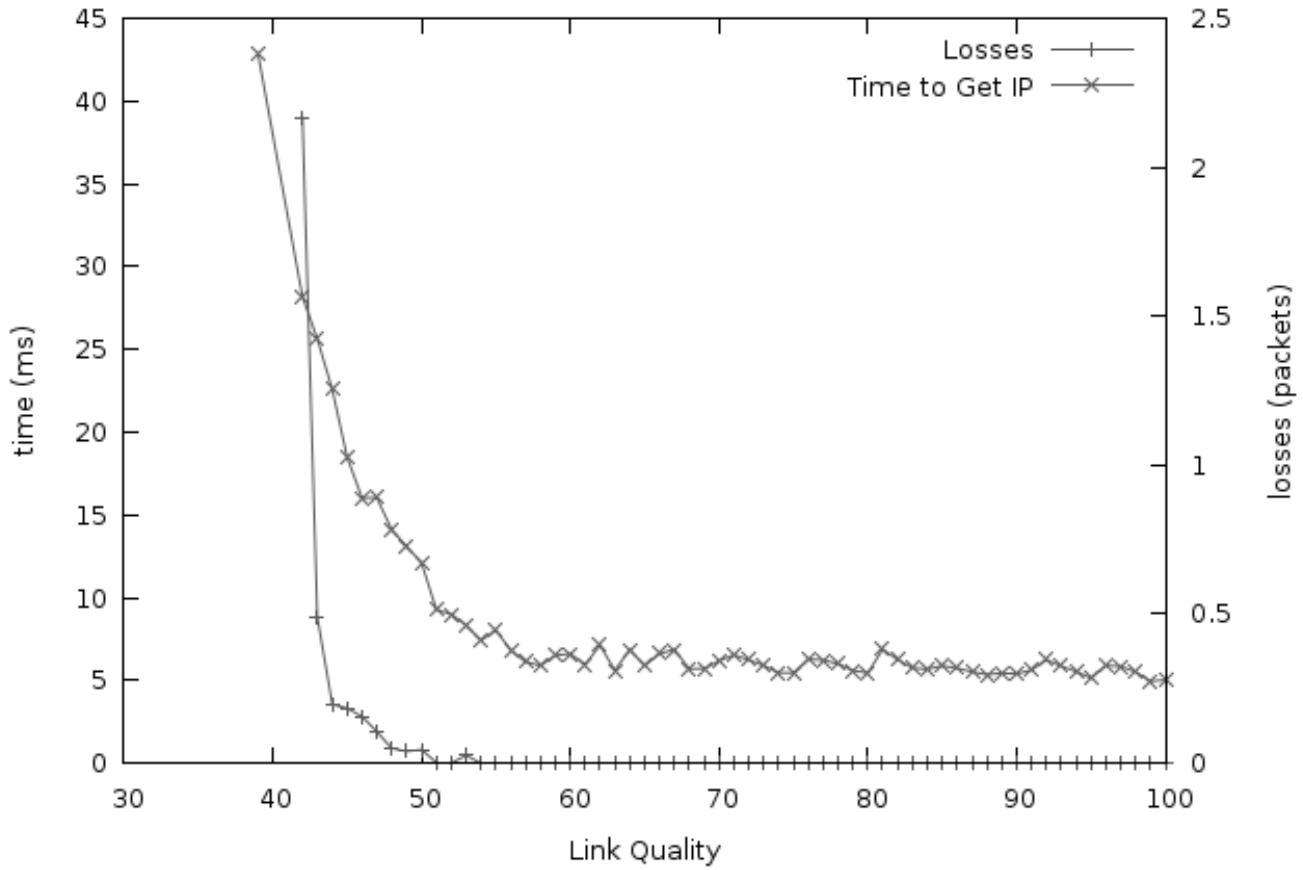


Figura 29.- Gráfica del tiempo en que tarda en asignarse una dirección IP y el número de pérdidas vs la calidad del enlace

Como se puede observar en la Figura 29, el tiempo de asignación de dirección IP se incrementa casi exponencialmente al disminuir la calidad del enlace (Link Quality). Por otra parte, al medir el desempeño del protocolo FDHCP, se observó que es liviano en memoria usando el 8% de la memoria total del AP. Por otra parte, en términos de procesador utilizó 80% del procesamiento del AP. Esto es debido a que el software usa threads, y analiza paquetes para mantener las direcciones activas. En cambio en el nodo móvil, resultó ser muy liviano usando sólo el 0.1% de procesamiento y el 1 % de memoria.

Los resultados muestran que se puede obtener una dirección IP en un tiempo de ida y vuelta (5ms), sin modificar la funcionalidad de DHCP. Además, durante la fase de experimentación no se presentaron casos de direcciones IP duplicadas. Por esa razón, la propuesta es confiable en la obtención de una dirección IP. De hecho, el FDHCP permite la coexistencia de ambos, sin necesidad de una modificación al servidor DHCP común.

4.2 FCLH: Fast Cross-Layer Handoff

El protocolo FCLH está basado en el paradigma básico Cliente-Servidor, en términos generales existen dos variantes, una proactiva y otra reactiva. Son muy parecidas, sólo cambia la implementación del mecanismo suavizador de pérdidas.

4.2.1 Plataforma de prueba

En este apartado se describe la topología de red que se usó para evaluar el desempeño de las propuestas FCLH, de igual manera de describen sus componentes. Durante el proceso de evaluación del protocolo se utilizó una sesión de video a la demanda con un servidor basado en RTSP para una sesión de video MPEGII. Debido a que la aplicación no soportaba movilidad en los clientes fue ligeramente modificada para soportarla, aprovechando la ventaja del código libre. Todos los sistemas tiene instalados, sistemas operativos LINUX o UNIX. La Figura 30 muestra una imagen del escenario de pruebas y a continuación se incluye una breve explicación de sus componentes.

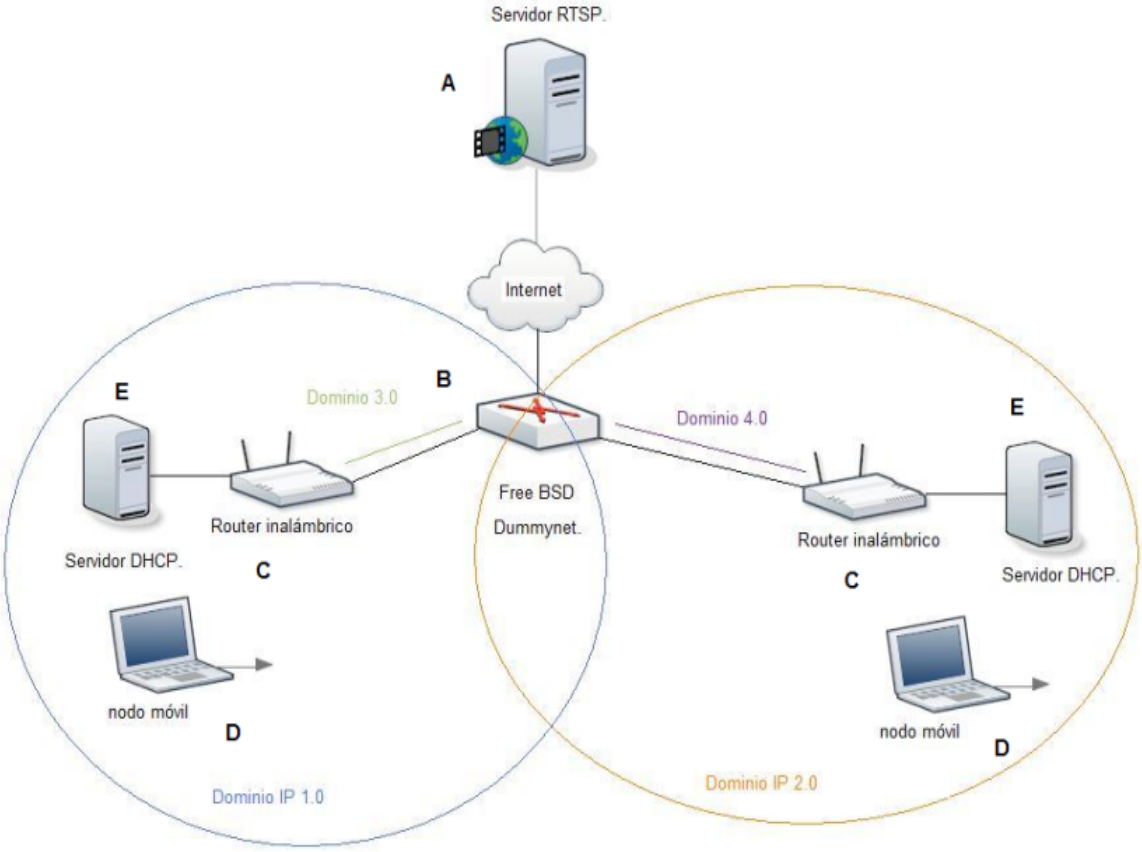


Figura 30.- Escenario de pruebas para protocolo FCLH.

A.- Servidor RTSP:

Es un servidor con procesador Centrino a 3 GHz , 1 GB de memoria RAM y tiene instalado un servidor de Video LIVE 555 Media server [74], este servidor en compatible con VLC player, Quick Time y open RTSP.

B.- Router Free BSD:

Es un servidor con sistema operativo Free BSD 8.0, que se comporta como router de frontera para los dos acces routers inalámbricos, este router de frontera contiene instalada la aplicación Dummynet[75], la cual sirvió para emular la distancia del servidor RTSP.

C.- Router inalámbrico:

Access Router inalámbrico con sistema operativo OpenWRT[55], memoria flash de 8 MB y 32 MB de RAM. Para poder compilar y ejecutar programas sobre los access routers, se utilizó un coss-compiler llamado Buildroot[76].

D.- Nodo Móvil:

El nodo móvil es una laptop con tarjeta inalámbrica. Durante las pruebas se probaron con varias laptops de diferente capacidad y variedad en tarjetas inalámbricas, todas ellas con sistema operativo Linux.

E.- Servidor DHCP:

El servidor DHCP es una computadora con sistema operativo fedora 9, 1GB de RAM y procesador pentium 4 a 2.5GHz, con un servidor DHCP instalado.

4.2.2 Servidor FCLH

Los objetivos del servidor FCLH son: 1)asignar una dirección IP rápida, 2)suavizar el número de paquetes perdidos y 3)mantener la continuidad de los servicios activos. Para cumplir los objetivos el servidor cuenta con tres módulos y todos se ejecutan simultáneamente al recibir un paquete DHCP *discover-o* para reducir la pérdida de paquetes y minimizar el tiempo de handover.

El módulo 1)**Servidor de Asignación de Direcciones IP Rápidas(FDHCP)** es el encargado de asignar una dirección IP rápida en un tiempo de ida y vuelta, el módulo 2)**Actualiza servicios** es el encargado de mantener activas las conexiones de los servicios establecidos previamente, el módulo 3)**Suavizador de pérdidas** es el encargado de disminuir la pérdida de mensajes durante la transición de red. El modulo suavizador de pérdidas cuenta con un sistema que reenvía el flujo de datos destinados al MN y existen dos implementaciones una para la propuesta reactiva y otra para la propuesta proactiva. Ambas implementaciones son ligeramente similares, aunque la principal diferencia radica en un buffer. Dicho buffer es usado por la propuesta proactiva para almacenar los datos antes de que cambie de red, acción que no realiza la propuesta reactiva.

El servidor FCLH se programó en lenguaje C, con ayuda de la librería LPCAP, haciendo uso de threads, para poder ejecutar varios módulos al mismo tiempo. La versión de firmware para los AP fue backfire y se compiló con el compilador cruzado Buildroot.

4.2.3 Cliente FCLH

El cliente será un software que se ejecuta en el MN y la función del cliente se limita a buscar redes, decidir a qué AP cambiar, conmutar físicamente de red y solicitar una dirección IP. Después de esas acciones está listo para continuar con sus sesiones activas, así como lo muestra el diagrama de flujo del cliente FCLH(véase, Figura 31). Debido a la complejidad de la programación, fue necesario hacer uso de código libre propuesto en la red. Es por eso que la implementación del cliente FCLH se desarrolló con el API Wireless Tools for Linux[77], sockets RAW, ioctl y todos los programas se escribieron en lenguaje C.

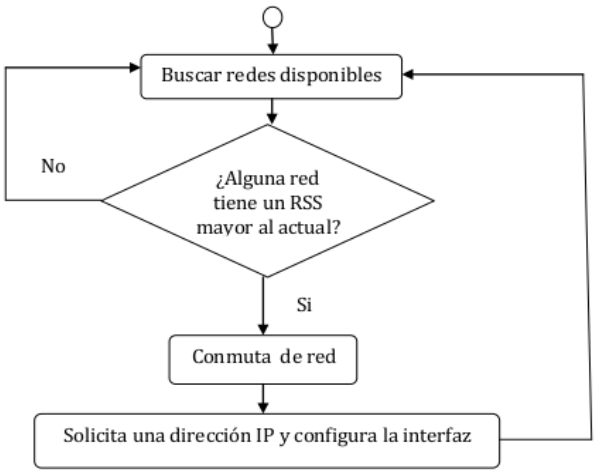


Figura 31.- Diagrama de flujo del cliente FCLH.

4.3 FCLH Reactivo

La propuesta reactiva toma acciones para mitigar los problemas del traspaso de red después de que se ha cambiado de red. Es decir, una vez asociado al nuevo AP, el MN solicita una nueva dirección IP. Entonces el MN envía un mensaje DHCP *discover-o* solicitando una dirección IP rápida y con este mensaje se desencadena el proceso de handover reactivo. Es decir, cuando el AP recibe el paquete DHCP *discover-o* se activan tres procesos.

1) Actualización de los servicios activos. En este caso se informa al servidor de video, incluyendo la actualización del Location Directory(directorio de ubicación).

2) Activación del servicio Smooth Handover. Es decir, activa un servicio que reenvía todo el flujo de datos destinado para el MN desde el AP viejo hasta la nueva red utilizando el mecanismo suavizador de pérdidas reactivo.
3) Otorgamiento de una dirección IP nueva al Nodo Móvil correspondiente al nuevo contexto. Este cometido se realiza con la respuesta al mensaje DHCP *discover-o*, emitiendo un mensaje DHCP *ack*¸ con la información necesaria para poder configurar la interfaz de red.

4.3.1 MSHO-R :Mecanismo suavizador de pérdidas reactivo

El proceso para suavizar las pérdidas durante un traspaso reactivo, básicamente consiste en solicitar al AP viejo, el flujo de datos dirigido al MN que aún está llegando al AP viejo. Debido a la naturaleza de la propuesta durante esta transición, existen pérdidas de paquetes.

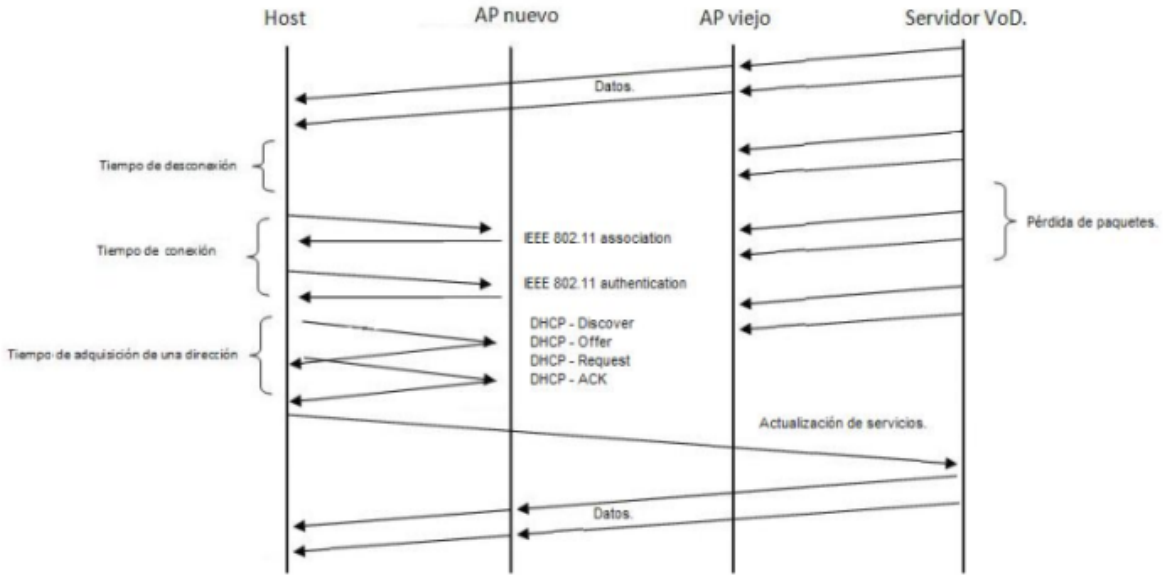


Figura 32.- Proceso de handover sin protocolo de movilidad.

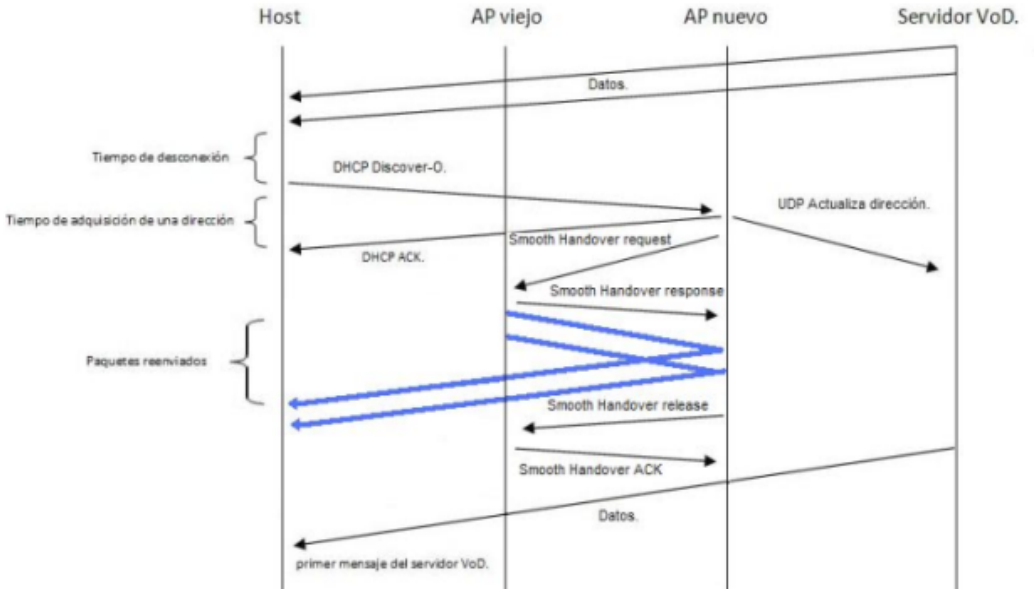


Figura 33.- Proceso de handover con FCLH.

Cuando el MN llega a la nueva red, envía un mensaje DHCP *discover-o. E*ntonces el servidor FCLH-reactivo envía cuatro mensajes al mismo tiempo. El primer mensaje DHCP *ack* se envía al MN con la configuración de red. El segundo mensaje es enviado al directorio de ubicación, informado la nueva dirección del MN. El tercer mensaje va dirigido al servidor VoD para que se redirija el flujo de datos a la nueva locación del MN. Por último, el mensaje Smooth Handover *request* va dirigido al AP viejo, solicitando el flujo de datos dirigido al MN. Entonces el AP viejo responde a la solicitud con un mensaje Smooth Handover *response* y comienza el reenvió de paquetes al nuevo AP. Cuando finaliza el reenvió de flujo de datos, el recurso debe ser liberado porque el proceso de reenvío de datos es costoso en términos de procesamiento de datos. Dicha acción la solicita el AP nuevo enviando un mensaje Smooth Handover *release* y una vez liberado el recurso, el AP viejo contesta la solicitud con un mensaje Smooth Handover *ack*.

4.3.2 Evaluación del desempeño

Las Figuras 34 y 35 muestran los resultados del tiempo de handover y el número de pérdidas por handover, en función del retraso de extremo a extremo entre el servidor de video a la demanda y el MN.

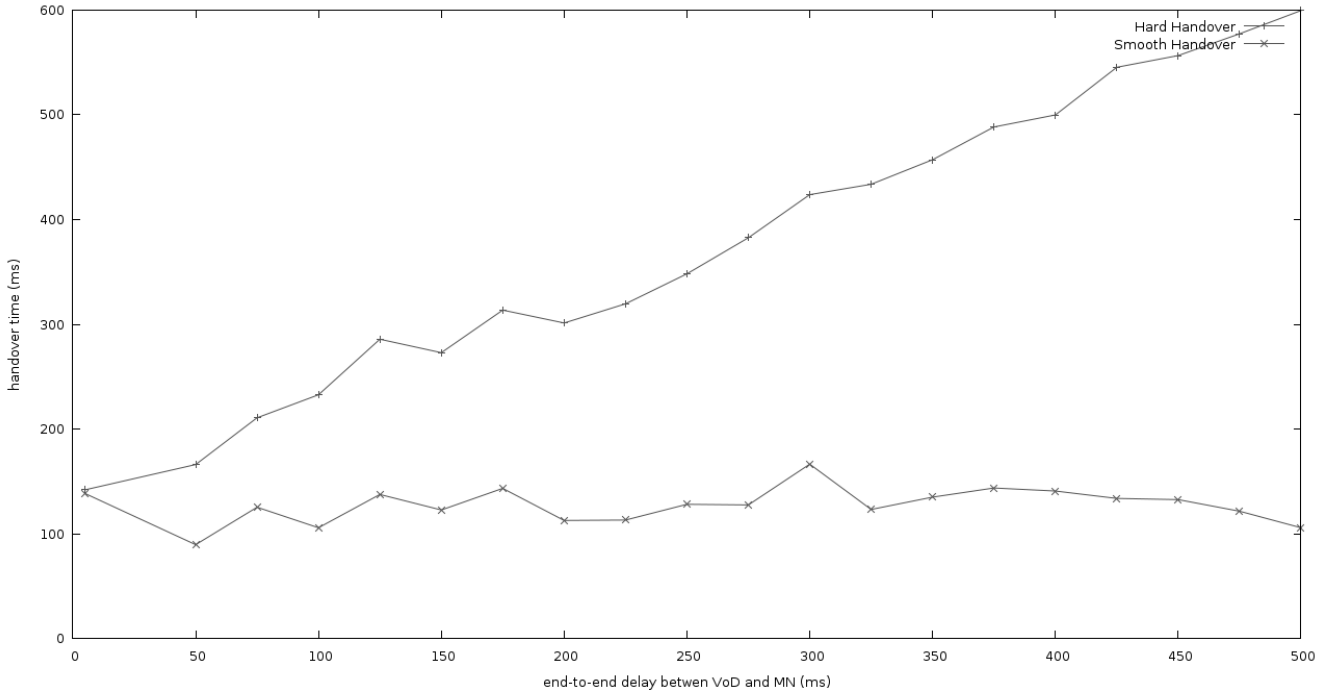


Figura 34.- Gráfica de tiempo de handover vs. retraso entre el MN y el CN

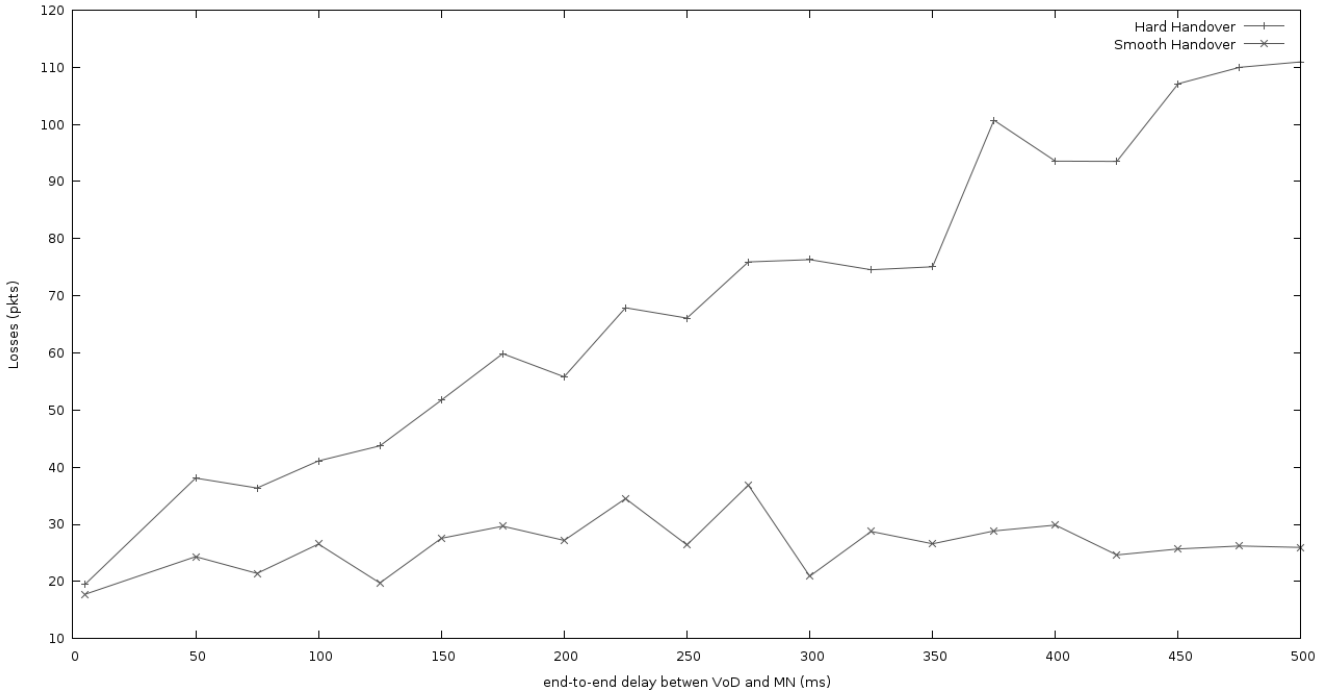


Figura 35.- Gráfica de paquetes perdidos vs. retraso entre el MN y el CN.

De las gráficas podemos observar que tanto el tiempo de handover y pérdidas no aumenta

para el smooth handover reactivo en función del retraso de extremo a extremo entre el MN y el CN, es decir se mantienen constante sin importar el retraso natural.

La gráfica que muestra la Figura 34, es proporcional a la gráfica analítica mostrada en la Figura 21. Por otra parte en el estudio analítico no se consideró que la propuesta se implementó a nivel usuario y no a nivel kernel. Esto aumenta el tiempo de handover, aunado a eso, existen tiempos a considerar como: el tiempo de configuración de la tarjeta de red, tiempo de asociación, entre otros. Todo esto genera un resultado mayor al analítico.

4.4 FCLH Proactivo

La propuesta proactiva toma acciones antes de que el MN cambie de red. Es decir, el MN informa al AP viejo que cambiará de red enviando un mensaje Seamless handover *request,* desencadenando así el proceso de handover. Entonces, el AP viejo comienza a guardar los paquetes dirigidos al MN, para reenviarlos posteriormente cuando el nuevo AP solicite los datos. Una vez que el MN cambie físicamente de red, debe solicitar una dirección IP rápida, enviando un mensaje DHCP *discover-o*, desencadenado el proceso de actualización de los servicios activos, el reenvió de paquetes y asignación de dirección IP. Esta propuesta ofrece mayor ventaja que la propuesta reactiva porque ofrece un handover seammless o un cambio de red sin fisuras, es decir no hay pérdida de paquetes, solamente desorden en los datos, debido a la concurrencia de los procesos.

4.4.1 MSHO-P :Mecanismo suavizador de pérdidas proactivo

El proceso suavizador de pérdidas, comienza cuando el MN envía un mensaje Seamless Handover *request* al AP actual. Entonces el AP comienza a almacenar los datos dirigidos al MN. Después de que el MN envía el mensaje Seamless Handover *request* informando que cambiará de red, el MN llega a la nueva red y debe solicitar una dirección IP válida. Entonces envía un mensaje DHCP *discover-o* y el AP nuevo solicita los datos almacenados al AP viejo con un mensaje Seamless handover *request*. Inmediatamente el AP viejo deja de almacenar datos, y simultáneamente ejecuta dos tareas. Por una parte, envía los datos almacenados y por otra, activa el reenvió de paquetes en caso de que sigan llegando datos.

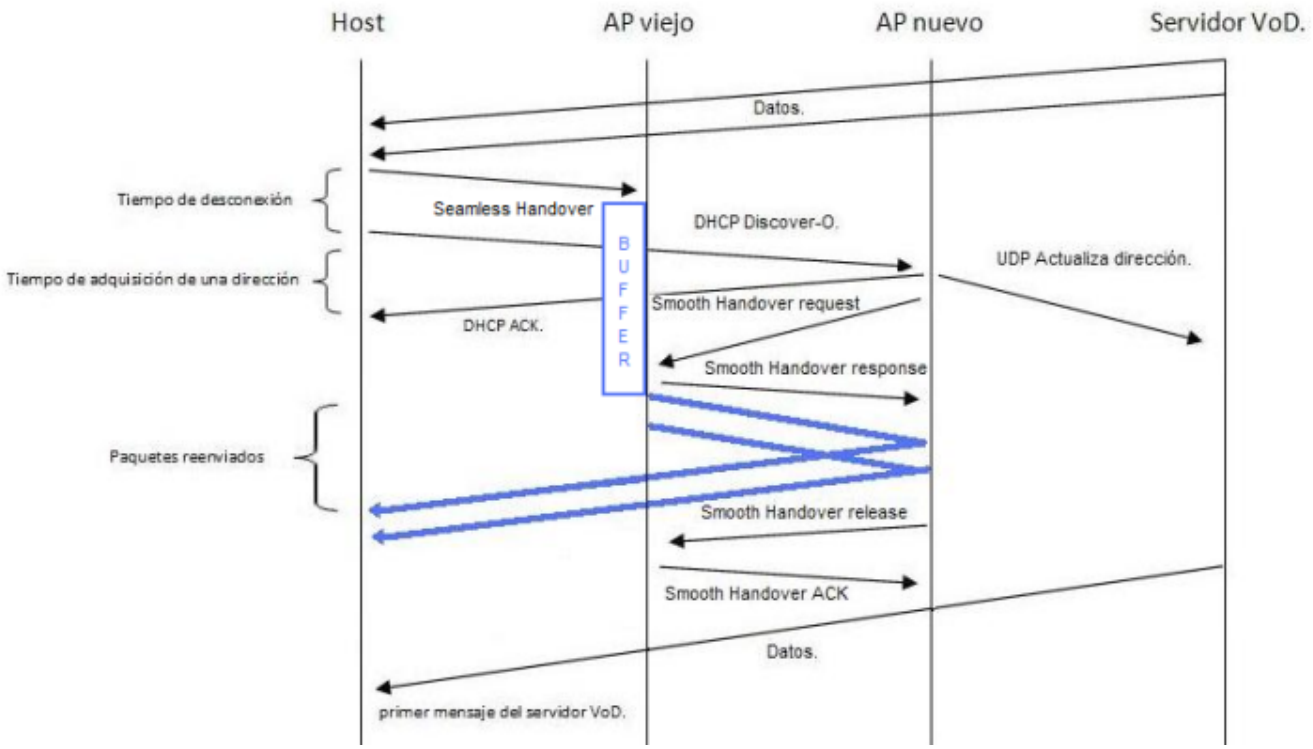


Figura 36.- Proceso de handover proactivo con FCLH.

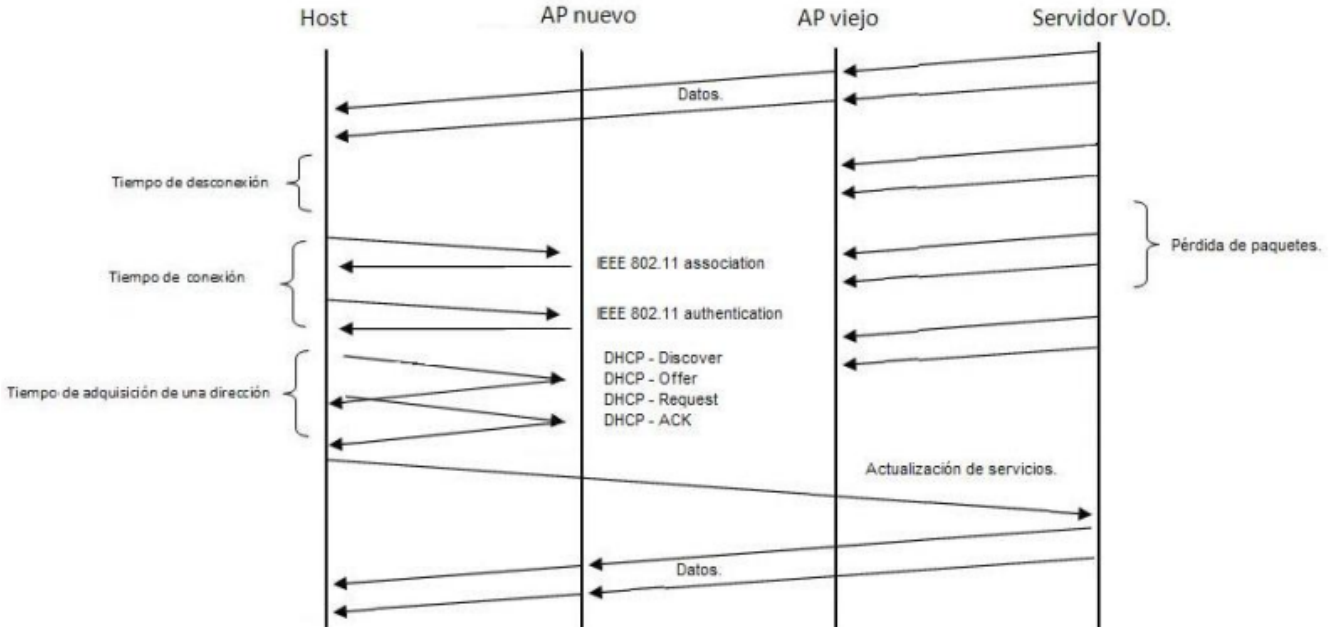


Figura 37.- Proceso de handover sin protocolo de movilidad.

4.4.2 Evaluación del desempeño

Las Figuras 38 y 39 muestran los resultados del tiempo de handover y el número de mensajes almacenados en el buffer por handover en función del retraso de extremo a extremo entre el servidor de video a la demanda y el MN.

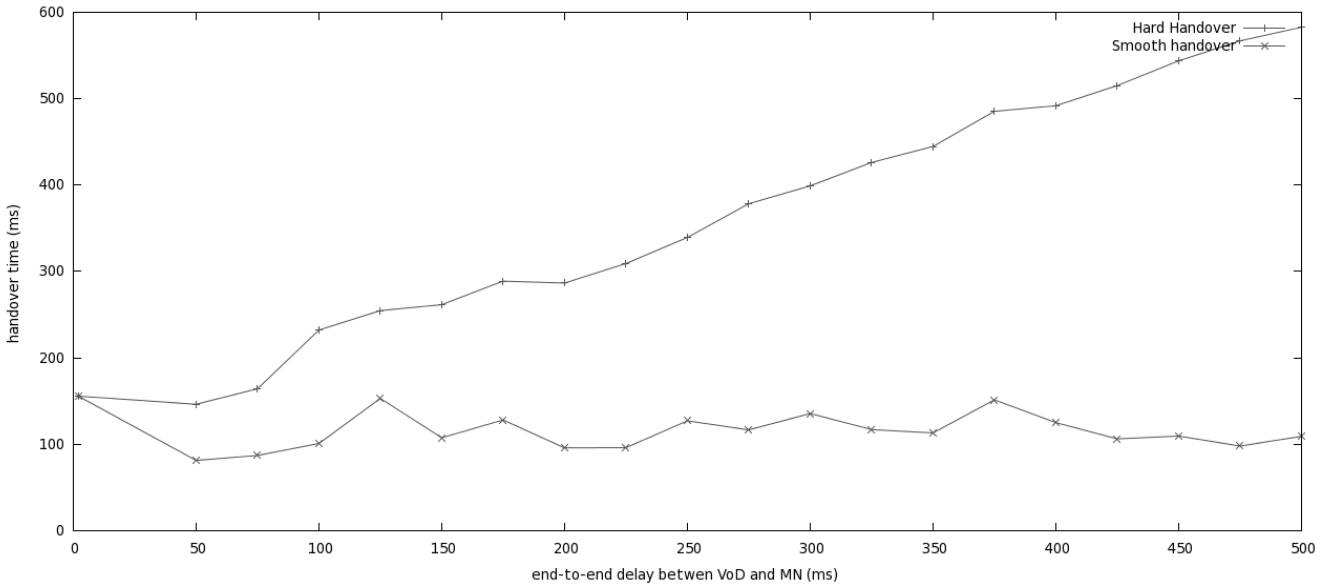


Figura 38.- Gráfica de tiempo de handover vs. retraso entre el MN y el CN.

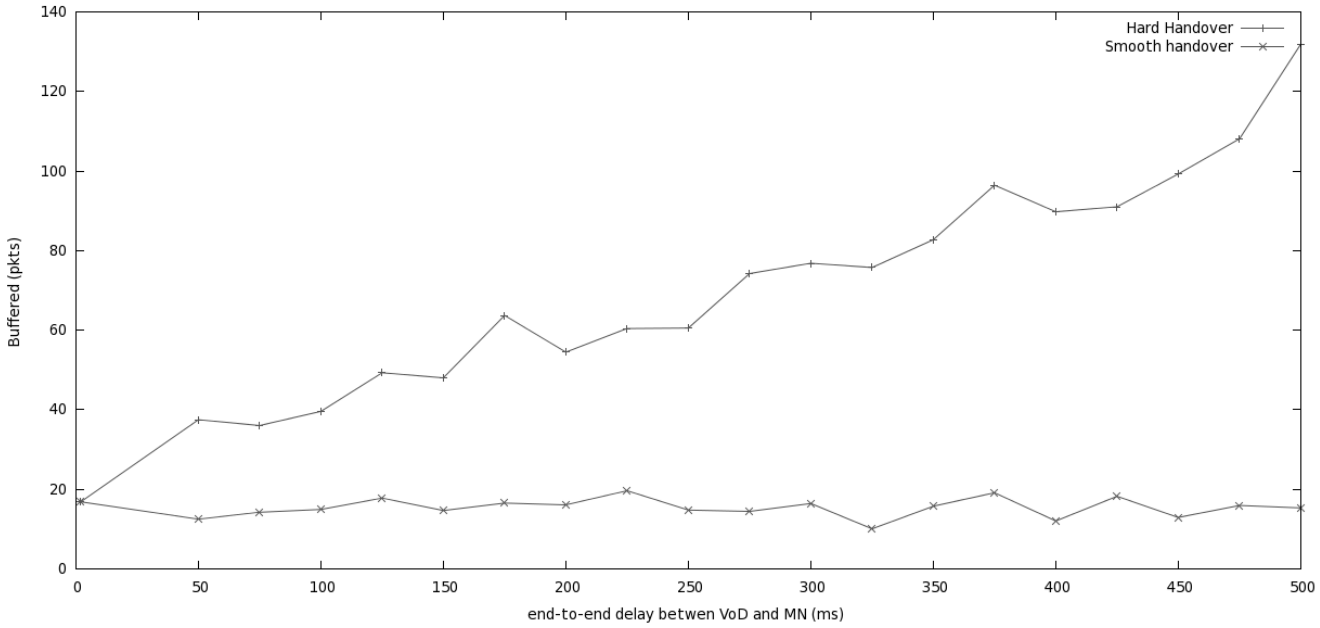


Figura 39.- Gráfica de paquetes almacenados en el AP vs. retraso entre el MN y el CN.

De las gráficas podemos observar que el tiempo del smooth handover proactivo no se incrementa al aumentar el retraso natural introducido por la distancia del CN. Asimismo, podemos observar que el número de paquetes almacenados en el buffer es constante sin importar el retraso de extremo a extremo entre el MN y el CN. Es decir, al realizar un handover proactivo, no hay paquetes perdidos en este esquema.

Por otra parte se consideró un flujo de datos de video, donde cada paquete en promedio contiene 1046.45 bytes. Como en promedio se almacenan 15.37 paquetes por handover, entonces multiplicado el número de paquetes por el número de bytes promedio por paquete, obtenemos el requerimiento promedio de memoria generando un total de 16083.93 bytes por handover, es decir 15.7KB. Se espera que cada nodo móvil salte en un tiempo distinto, por lo tanto la gráfica no es proporcional al número de nodos móviles.

Finalmente existe una gran diferencia entre las propuestas implementadas y las simuladas, porque en la bibliografía no se consideran los cambios de contexto. Es decir, en la tabla 1, podemos apreciar que en las implementaciones de hadover son más costosas en términos de tiempo, oscilando entre los 100 y 1000 milisegundos, como se puede apreciar en la Figura 40. Asimismo, se realiza una comparación en términos de porcentaje de pérdidas en la Figura 41.

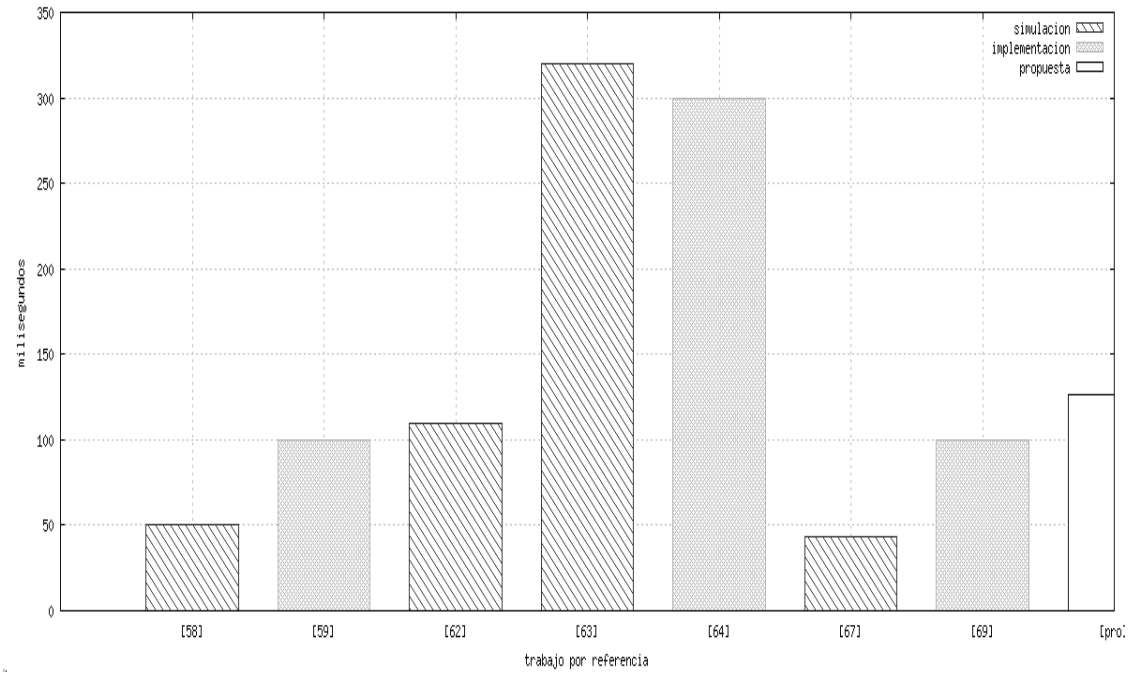


Figura 40.- Gráfica comparativas de propuestas en términos de tiempo

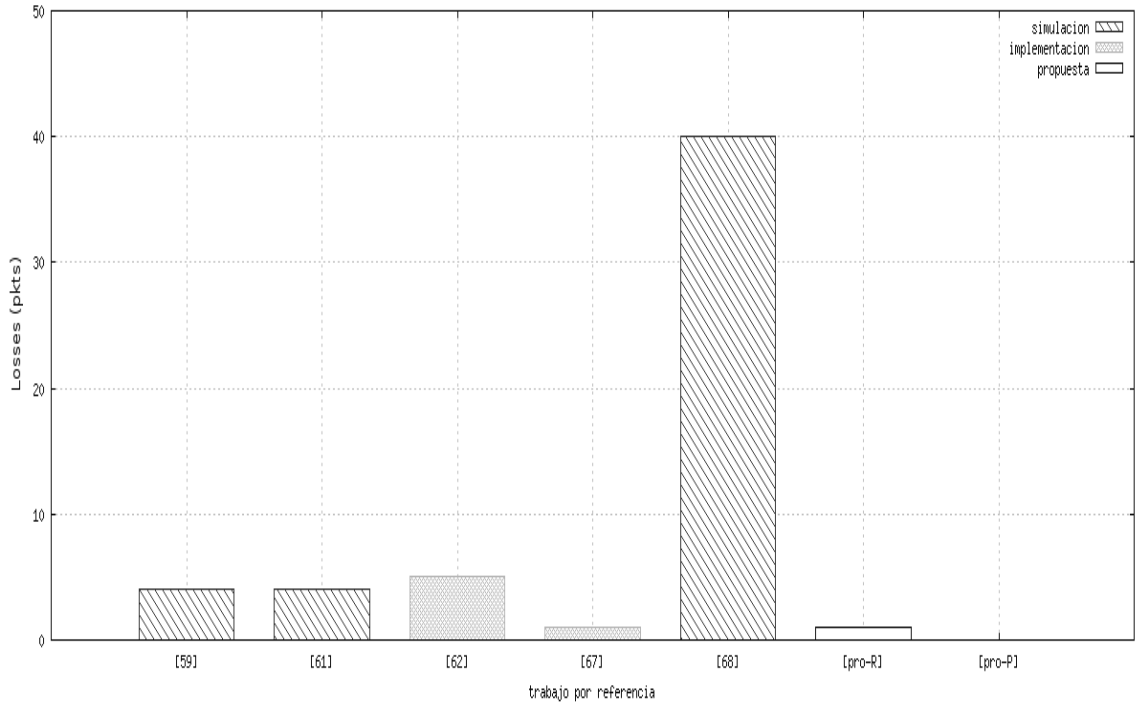


Figura 41.- Gráfica comparativa de propuestas en términos de porcentaje de pérdidas

5 Conclusiones y trabajo futuro

Los resultados muestran un handover seamless logrando un cambio de red en un tiempo promedio de **126.8709588** ms, para la implementación reactiva. En contraparte la implementación proactiva muestra un handover sin pérdidas de paquetes, logrando almacenar en el buffer **15.3729619** paquetes por hadover en promedio. Por otra parte se implementó un protocolo de adquisición de direcciones rápido logrando obtener una dirección en un tiempo promedio de **75.3729189** ms, también se observó un incremento exponencial en el tiempo de adquisición de una dirección IP en función de la potencia de la señal, es por eso que se recomienda realizar un salto con una potencia superior a -40 db o 60 % de Quality of Link.

La implementación de procesos paralelos resultó ser muy costosa en términos de procesamiento debido a que se implementó con hilos consumiendo el 80 % de procesador, pero por otra parte el consumo de memoria fue bajo, consumiendo el 1% de memoria. Observando la gráfica del tiempo de handover vs. retardo de extremo a extremo, la ventaja del protocolo se vuelve clara a partir de 50 ms de retardo de extremo a extremo entre el CN y el MN, manteniendo un tiempo de salto casi constante sin importar la distancia de los servidores a diferencia del tiempo de Handover hard en el que su latencia es directamente proporcional al retardo de extremo a extremo entre el MN y los servicios activos.

Considerando el desempeño del smooth handover en cuestión de pérdidas fue muy satisfactorio minimizando las pérdidas logrando un handover seamless, para la propuesta proactiva. Sin embargo la apertura y cerrado de sockets es costosa en cuestión de tiempos es por eso que los sockets se mantuvieron abiertos todo el tiempo y siempre listos para transmitir o recibir. Las variaciones de la gráfica son causadas por el enlace inalámbrico y las múltiples interferencias debido a que se realizó en un entorno universitario, donde hay muchos puntos de acceso. Sería recomendable que los AP de salto tuvieran un canal distinto, sin traslapes, para así obtener una gráfica más suave, sin tantos picos. Por otra parte, resultó que el procesamiento de paquetes en el AP resultó no ser tan rápido. Esto debido a la implementación con lpcap ocasionado porque se debía de realizar una copia del

paquete para ser modificado y reenviado puesto que el área de almacenamiento está protegida por el sistema operativo y no se podía modificar.

Por otra parte nuestra propuesta es muy ligera en términos de modificaciones de las capas protocolarias, además los nodos modificados permiten interactuar con otros sin problema alguno. También la propuesta es muy poco invasiva en comparación con las otras propuestas citadas en la bibliografía, en términos de arquitectura e infraestructura protocolaria donde se tienen que incluir, servidores proxy, modificaciones a capas completas, etc.
Nuestra propuesta permite escalabilidad sin problemas debido a que el buffer en la propuesta proactiva almacena en promedio **15.7KB**, considerando que el sistema cuenta con una memoria RAM de **32MB**, en teoría podría atender hasta **2038** usuarios.

En este trabajo se implantó el protocolo FCLH, pero se considerará posteriormente evaluar la propuesta con métodos como PSNR y SSIM, para observar la calidad del video, en términos de tasa de pérdidas, retardo de extremo a extremo, jitter, etc.

6 Referencias

1. W. Stevens. UNIX Network programming. Prentice Hall
2. M. Handley, H. Schulzrinne, E. Schooler, and J. Rosenberg. SIP: Session Initiation Protocol. rfc 2543, IETF, March 1999.
3. C. Perkins, "IP Mobility Support", RFC 2002, Internet Engineering Task Force, October 1996 .
4. A. C. Snoeren and H. Balakrishnan, "An End-to-End Approach to Host Mobility", 6th IEEE/ACM Mobicon 2000. Boston, August 2000.
5. Aggeliki Sgora , Dimitrios D. Vergados , “Handoff Prioritization and Decision Schemes Survey”, ieee communications surveys & tutorials, vol. 11, no. 4, fourth quarter 2009
6. Mohamed Alnas, Irfan Awan, R Holton , “A Survey of Handoff Performance in Mobile IP” , Third UKSim European Symposium on Computer Modeling and Simulation , 2009.
7. Nokia, “Mobile VOIP: IP Convergence Goes Mobile“ . Nokia network 2005
8. RFC 3753 Mobility Related Terminology , J. Manner, M. Kojo, June 2004
9. Giorgos Karopoulos, Georgios Kambourakis, And Stefanos Gritzalis, “survey of secure handoff optimization schemes for multimedia services over all-ip wireless heterogeneous networks ”, IEEE Communications surveys, 3rd quarter 2007, volume 9, no. 3 .
10. Part11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE Std. 802.11, 1999.
11. Yong Liao, Lixin Gao , Practical Schemes for Smooth MAC Layer Handoff in 802.11 Wireless Networks , Proceedings of the 2006 International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM'06)
12. A. Mishra, M. Shin, and W. Arbaugh. An empirical analysis of the IEEE 802.11 MAC layer handoff process. SIGCOMM Comput. Commun. Rev., 33(2):93–102, 2003.
13. Chung-Sheng Li , Yung-Chih Tseng, Han-Chieh Chao, Yueh-Min Huang “ A neighbor caching mechanism for handoff in IEEE 802.11 wireless networks ” , The Journal of Supercomputing July 2008, Volume 45, Issue 1, pp 1-14.

14. Mahnsuk Yoon, Keuchul Cho, Jilong Li, Jeongbae , Yun, Minyoung Yoo, Youngil Kim, Qin Shu and JangKyu Yun , “AdaptiveScan: The Fast Layer-2 Handoff for WLAN ”, 2011 Eighth International Conference on Information Technology: New Generations .
15. Timucin Ozugur and Behcet Sarikaya, «Fast IPv4/IPv6 Address Acquisition in Wireless LANs,» de Consumer Communications and Networking Conference, 2004. CCNC 2004. First IEEE Jan 2004.
16. André Zúquete , Carlos Frade, «Pre-allocation of DHCP leases: a cross-layer approach,» de International Conference on New Technologies, Mobility and Security (NTMS), Feb. 2011.
17. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, IEEE IETF, 2012.
18. Bob O'hara, Al Petrick, “IEEE 802.11 handbook a designer's companion”, second edition, New York : IEEE, 2004.
19. I. Ramani and S. Savage, “SyncScan: Practical fast handoff for 802.11 infrastructure networks.” In Proc. 24th INFOCOM, Mar. 13- 17, 2005, vol. 1, pp.675-684.
20. Y. Chen, M. Chuang and C. Chen, “DeuceScan: Deuce-Based Fast Handoff Scheme in IEEE 802.11 Wireless Networks.” IEEE Transactions on Vehicular Technology, Vol. 57, pp.1126-1141, Mar. 2008.
21. D. Johnson, C. Perkins, and J. Arkko, "RFC 3775 -Mobility Support in, IPv6," IETF Networking Group,June 2004.
22. B. Hamdaoui and P. Ramanathan, “A Network-Layer Soft Handoff Approach for Mobile Wireless IP-Based Systems”, IEEE journal, vol. 22, no 4, MAY 2004 .
23. D. Lee, G. Hwang, and C. OH, (Performance enhancement of Mobile IP by educing out-of-sequence packets using priority scheduling, IEICE Transaction Communication), Vol E85-B, August 2002
24. K. El Malki, “Low Latency Handoffs in Mobile IPv4”, Internet Draft, Network Working Group, 2006 .
25. Mohamed Alnas, Irfan Awan, D.R Holton , “Handoff Mechanism in Mobile IP ”,
26. Robert Hsieh, Zhe Guang Zhou, Aruna Seneviratne , “S-MIP: A Seamless Handoff Architecture for Mobile IP ”, INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications. IEEE Societies (Volume:3), 2003.
27. H. Chaouchi and P. Antunes, ”Pre-handover Signaling for QoS Aware Mobility Management,” International Journal of Network Management, No. 14, pp.367-374, 2004.

28. Y. Bi, P. Iyer, ”An Integrated IP-layer Handover Solution for Next Generation IP-based Wireless Network”, IEEE Vehicular Technology Conference VTC2004-Fall, Vol. 6, pp.3950-3954, Los Angeles, USA, 2004
29. R. Hsieh and A. Seneviratne, “Performance analysis on Hierarchical Mobile IPv6 with Fast-handoff over TCP,” in Procedings of GLOBECOM, Taipei, Taiwan, 2002.
30. C. Techabanyat, and W. Benjapolakul, “Distributed Local Paging Scheme for Mobility Management in Mobile IP,” in Proc, APCC 2007, p. 265-269.
31. J. Xie, “User Independent Paging Scheme for Mobile IP,” Wireless Networks, vol. 2, pp. 145-158, 2006.
32. K. Hong, H. Jung, and S. Lee, “Cost-Effective IP Paging for Wireless Internet,” in Proc. IEEE Globecom 2007, p. 1982-1986.
33. Anyamanee Navichai, Watit Benjapolakul , “Two-Step Paging for Reducing Signaling Costs in Mobile IP ”, 13th International Conference on Advanced Communication Technology (ICACT), Seoul Febrero 2011.
34. Nilanjan Banerjee, et al. “Mobility Support In Wireless Internet ”, Wireless Communications, IEEE, Volume:10 , Issue: 5 , page 54-61. October 2003.
35. A. C. Snoeren and H. Balakrishnan, “An End-to-End Approach to Host Mobility,” Proc. 6th Int’l. Conf. Mobile Comp. and Net., Boston, MA, Aug. 2000.
36. Bill Croft, John Gilmore, BOOTSTRAP PROTOCOL (BOOTP), RFC 951.
37. R. Droms, “RFC 2131 Dynamic Host Configuration Protocol”, March 1997.
38. E. Wedlund and H. Schulzrinne, “Mobility support using SIP”, de ACM/IEEE WoWMoM’99, Seattle, USA, Aug 1999.
39. A. G. Forte, S. Shin, and H. Schulzrinne, «Passive Duplicate Address Detection for Dynamic Host Configuration Protocol (DHCP),» Columbia University., March 2006..
40. Timucin Ozugur and Behcet Sarikaya, «Fast IPv4/IPv6 Address Acquisition in Wireless LANs,» de Consumer Communications and Networking Conference, 2004. CCNC 2004. First IEEE Jan 2004.
41. André Zúquete , Carlos Frade, «Pre-allocation of DHCP leases: a cross-layer approach,» de International Conference on New Technologies, Mobility and Security (NTMS), Feb. 2011.
42. W. Simpson , “IP in IP Tunneling RFC 1853”, October 1995.
43. B. Storer and et al, “Softwire Hub and Spoke Deployment Framework with L2TPv2,” RFC5571, IETF, June 2009.
44. C. Borman and et al, “Robust Header Compression:Framework and four profiles:RTP, UDP, ESP, and uncompressed,” RFC3095, July 2001.
45. V. Jacobson, “Compressing TCP/IP Headers,” RFC1144, Feb. 1990.
46. M. Degermark and et al, “IP Header Compression,” RFC2507, 1999.
47. Bremler-Barr, A, Levy, H.”spoofing prevention method”, INFOCOM 2005. 24th Annual

Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, 536 - 547 vol. 1, 2005.

48. D. Bruschi, A. Ornaghi, and E. Rosti, “S-ARP: A secure address resolution protocol,” 19th Annual Computer Security Applications Conference, pp. 66-74, Nevada, USA, 2003
49. M. V. Tripunitara, and P. Dutta. “A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning,” Proceedings of the 15th Annual Computer Security Application Conference (ACSAC), pp. 303-309, 1999.
50. Biju Issac , Secure ARP and Secure DHCP Protocols to Mitigate Security Attacks , International Journal of Network Security, Vol.8, No.2, PP.107–118, Mar. 2009
51. J. loannidis and S. Bellovin., “Implementing pushback: Router-based defense against ddos attacks.” in Proc. NeWoIJI curd Distributed System Securiry Symposium,Cufifonliu.February 2002.
52. D. Song and A. Perrig, “Advanced and authenticated marking schemes for ip traceback,” in Pmc. IEEE JNFOCOM. 2001
53. T. Komori, and T. Saito, “The secure DHCP system with user authentication,” Proceedings of the 27th Annual IEEE Conference on Local Computer Networks (LCN), pp. 123-131, Florida, USA, 2002.
54. C. M. Kozierok, The TCP/IP Guide Website, 2005. (http://www.tcpipguide.com/free/ARPMessageFormat.htm)
55. OpenWrt Backfire 10.03.1-RC6 | Load: 1.95 1.60 0.89, [Online]. Available:http://openwrt.org
56. Internet System Consortium (ISC). Dynamic Host Configuration Protocol (DHCP). dhcp-.0.3. [Online]. Available: http://www.isc.org
57. Park, S., Kim, P., and Volz, B., "Rapid Commit Option for the Dynamic Host Configuration Protocol version 4 (DHCPv4)," RFC4039, IETF, March 2005.
58. Jen-Jee Chen, Yu-Chee Tseng, and Hung-Wei Lee, "A Seamless Handoff Mechanism for DHCP-Based IEEE 802.11 WLANs", IEEE COMMUNICATIONS LETTERS, VOL. 11, NO. 8, AUGUST 2007
59. Eunchul Cha, Kyounghee Lee, Myungchul Kim, Cross Layer Fast Handoff for SIP, 21st

International Conference on Advanced Networking and Applications(AINA'07).

60. mohammed boutabia, hossam afifi, collaborative handover mechanism for real-time services, 9th International Conference on Intelligent Transport Systems Telecommunications,(ITST),2009.
61. Gurpal Singh, Ajay Pal Singh Atwal, B.S. Sohi,Multimedia Ready Handoff Technique for 802.11 Networks, 15th International Conference on Advanced Computing and Communications.
62. Tarik Taleb∗ , Tomoyuki Nakamura, and Kazuo Hashimoto, On Supporting Handoff Management for Multi-Source Video Streaming in Mobile Communication Systems,
63. Nashaat, H., Rizk, R.,Mahdi, H., Performance Analysis of Streamed Video Over Mobile IP Based Networks, 9th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA), 2011.
64. Andre Zuquete Carlos Frade, Pre-allocation of DHCP leases: a cross-layer approach
65. Claudio de Castro Monteiro, Paulo Roberto de Lira Gondim, Vinicius de Miranda Rios, Alex Coelho, Stéphany Moraes Martins, Video session handoff between WLANs, ICACT'10 Proceedings of the 12th international conference on Advanced communication technology Pages 1203-1208, 2010.
66. Sheu, Tsang-Ling, Video Stream Splitting and Merging using Dual Mobile-IP Tunnels in Wireless Handoffs,Telecommunications: The Infrastructure for the 21st Century (WTC), 2010.
67. P. Machań and J. Wozniak, A Lightweight Algorithm for Fast IEEE 802.11 Handover, Telecommunication Networks and Applications Conference (ATNAC), 2012 Australasian.
68. Saleh Abdallah-Saleh, Qi Wang, Christos Grecos and Duncan Thomson, Handover Evaluation for Mobile Video Streaming in Heterogeneous Wireless Networks
69. Mellimi, S., Location Base Fast MAC handoffs in 802.11,International Conference on Wireless, Mobile and Multimedia Networks, 2008. IET, 11-12 Jan. 2008
70. B. Jooris, A. Schoutteet, F. Vermeulen. and I. Moerman, Access network controlled fast handoff for streaming multimedia in WLAN, Mobile and Wireless Communications Summit, 2007. 16th IST.

71. Feng-Yi Chou, I-Ju Liao, Ya-Chun Li, Tin-Yu Wu, Wei-Tsong Lee, A pre-registered Handoff scheme in IEEE 802.11r Wireless Local Area Networks, 2010 International Conference on Communications and Mobile Computing.
72. Sourav Pal , Sumantra Kundu , Preetam Ghosh , Kalyan Basu , and Sajal Das. A Framework for Fast Handoff in IEEE 802.11 Based Systems.
73. M. Karam and F. Tobagi. Analysis of the Delay and Jitter of Voice Traffic over the Internet. In Proceedings of IEEE INFOCOM'01, Anchorage, AL, April 2001.
74. LIVE555 Streaming Media, [Online]. Available:http://www.live555.com/liveMedia/
75. Marta Carbone and Luigi Rizzo, Dummynet Revisite, ACM SIGCOMM Computer Communication Review, 40(2) pg.12-20, March 2010
76. Buildroot, [Online]. Available: http://buildroot.uclibc.org/
77. Wireless Tools for Linux - Hewlett Packard 74. [Online]. Available: http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Tools.html
78. Andrew T. Campbell, Javier Gomez, Sanghyo Kim, András G. Valkó, Chieh-Yih Wan and Zoltán R. Turányi, " Design, Implementation, and Evaluation of Cellular IP ", journal IEEE Personal Communications, 2000, volume 7, pages 42-49.
79. A. G. Valko, "Cellular IP: A New Approach to Internet Host Mobility," ACM Comp. Commun. Rev., Jan. 1999.
80. A. Campbell et al., "Cellular IP," Internet draft, draft-ietf-mobileip-cellu-larip-00.txt, Dec. 1999; work in progress.

Casa abierta al tiempo

PC y TI

UNIVERSIDAD AÚTONOMA METROPOLOTNA – IZTAPALAPA
DIVISION DE CIENCIAS BÁSICAS E INGENIERIA

Infraestructura ligera para soportar video streaming sin fisuras en ambientes móviles WLAN

Tesis que presenta
Josué Vicente Cervantes Bazán
Para obtener el grado de
Maestro en Ciencias y Tecnologías de la Información

Asesor: Dr. Luis Martín Rojas Cárdenas, UAM-I.

Jurado Calificador:

Presidente: Dr. Javier Gómez Castellanos
Secretario: Dr. Miguel López Guerrero.
Vocal: Dr. Luis Martín Rojas Cárdenas

México, D.F. Enero 2014.