# MODELADO Y SIMULACIÓN DEL PROTOCOLO MOIP EN LA HERRAMIENTA DE SOFTWARE QUALNET

RAÚL ESTEBAN RESTREPO RHENALS

GERSON SALINAS VOGEL

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA

CARTAGENA

2011

# MODELADO Y SIMULACIÓN DEL PROTOCOLO MOIP EN LA HERRAMIENTA DE SOFTWARE QUALNET

RAÚL ESTEBAN RESTREPO RHENALS

GERSON SALINAS VOGEL

Monografía para optar titulo de profesional en programa académico

Asesor:

Ricardo Javier Arjona Angarita

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

FACULTAD DE INGENIERÍA

CARTAGENA

2011

**Nota de aceptación:**

_____

_____

_____

_____

_____

_____

_____

**Jurado**

_____

**Jurado**

**Cartagena de Indias Julio de 2011**

CONTENIDO

PAG

LISTA DE FIGURAS

PAG

LISTA DE ANEXOS

PAG

# ACRÓNIMOS

**MN:** Nodo Móvil

**FA:** Foreign Agent

**HA:** Home Agent

**IP:** Internet Protocol

**ICMP:** Internet control message protocol

**CN:** Nodo Correspondiente

**MoIP:** Mobile IP

**CoA:** Care-Of Address

# GLOSARIO

**Nodo Móvil (MN):** un host que tiene la capacidad de desplazarse y cambiar su punto de acceso respecto a una red.

**Care-Of Address:** dirección IP temporal de un nodo móvil mientras visita una red foránea.

**Home Address:** dirección IP de un Nodo Móvil mientras se encuentra en su red domestica.

**Nodo correspondiente (CN):** un nodo en la nube IP que se comunica con el MN.

**Foreing Agent (FA):** Router de una red visitada.

**Home Agent (HA):** Router de una red domestica.

**Mobility Binding:** asociación de una dirección IP aun MN mientras permanece en un enlace.

**Registro:** Proceso por el cual un MN solicita que se actualice su Mobility Binding para cambiar su punto de enlace.

**Roaming:** capacidad de un dispositivo de moverse de un punto de cobertura a otro.

**Handover:** capacidad de una red de mantener la transferencia de datos aunque se cambie el punto de enlace.

RESUMEN

El aumento y desarrollo de redes móviles e inalámbricas ha sido dirigido mayormente a las redes IP, sugiriéndose para ello a MoIP (Mobile IP) como el estándar global para la macro movilidad, lo que deja suponer que el futuro escenario de las redes inalámbricas será dominado por Mobile IP. Para una correcta comprensión y un apropiado análisis del protocolo, es necesario sentar bases rígidas y buscar herramientas competentes que permitan realizar comparaciones, visualización y obtención de datos que contengan información valiosa. Por tal motivo se optado por usar el software de simulación *Qualnet*, el cual reúne todas las características anteriormente descritas, permitiendo implementar diferentes escenarios con diferentes modelos de propagación con el fin de evaluar diversas condiciones. En este documento se describe de manera secuencial el funcionamiento de protocolo MoIPv4, así como la simulación de distintos escenarios que contengan los elementos propios de una red móvil.

# OBJETIVOS

- Exponer los aspectos más relevantes sobre Mobile IP y algunos problemas inherentes.

- Describir la filosofía de diseño de cada uno de los modelos de simulación de las entidades de Mobile IP.

- Comparar los diferentes escenarios que se presentan en el entorno real de las redes móviles mediante resultados estadísticos.

- Proponer el estudio y desarrollo de aplicaciones basadas en movilidad IP como parte de la formación en el área de comunicaciones del departamento de ingeniería electrónica de la UTB.

# INTRODUCCIÓN

El protocolo para la movilidad IP (Mobile IP) fue desarrollado con el fin de proporcionar un enrutamiento de datagramas hacia Host móviles sin presentar fisuras en el proceso. Detrás de este supuesto, MoIP debería ser capaz de trabajar bajo la infraestructura existente de internet basada en el protocolo TCP/IP, el cual fue desarrollado originalmente para redes fijas. Este reto fue poco a poco superado y MoIP se proyecta como el protocolo dominante de la movilidad IP.

En la actualidad, la mayoría de las actividades humanas están basadas en la utilización de la gran nube de internet, esto no es más que el envió de paquetes de un Host a otro en internet. Cada Host está identificado por una única dirección IP que consiste en identificador de red y de Host. Los datagramas IP son direccionados hasta la red en que se encuentra el Host de destino, luego este Host envía un datagrama como respuesta (ACK) hacia el Host de origen. Pero ¿qué sucede cuando un usuario con una única dirección IP dentro de una red inalámbrica desea comenzar a moverse y probablemente salir del área de cobertura?, seguramente el usuario intentara conectarse con esa misma dirección IP a la red más cercana lo que resultara con una conexión fallida. MoIP resuelve este inconveniente otorgando a los Hosts y Router la capacidad de enviar paquetes de una localización a otra de manera transparente.

Con el fin de aprovechar al máximo el desarrollo de las redes IP de nueva generación y evitar altos costos debido a errores de diseño, es muy importante evaluar detalladamente MoIP y los protocolos relacionados para los diferentes escenarios o condiciones de operación que podrían presentarse en la inminente nueva generación de internet móvil. Es por eso que este documento describimos la implementación de un modelo de simulación de Mobile IP. Este modelo incluye un número de características avanzadas para Mobile Ip, como son:

- Detección de movimiento.
- Multicast - Handover.
- Operación de registro.
- Tunneling.

El resto del documento fue organizado de manera que se guie de manera clara hacia los conceptos ligados a este importante protocolo.

# 1. INTRODUCCIÓN A MOIP V4

Mobile IP (MoIP) permite a los usuarios moverse libremente (Roaming) más allá de su red familiar mientras mantiene su dirección IP. Esto permite un enrutamiento transparente de los datagramas IP a los usuarios móviles (MN) durante su movimiento, tal que se puedan iniciar sesiones, de igual manera, las sesiones que ya han sido iniciadas antes del movimiento pueden ser mantenidas. El proceso que permite la conmutación de una red a otra se conoce como "Handover", sobre este término se tratara más profundamente en las secciones subsiguientes.

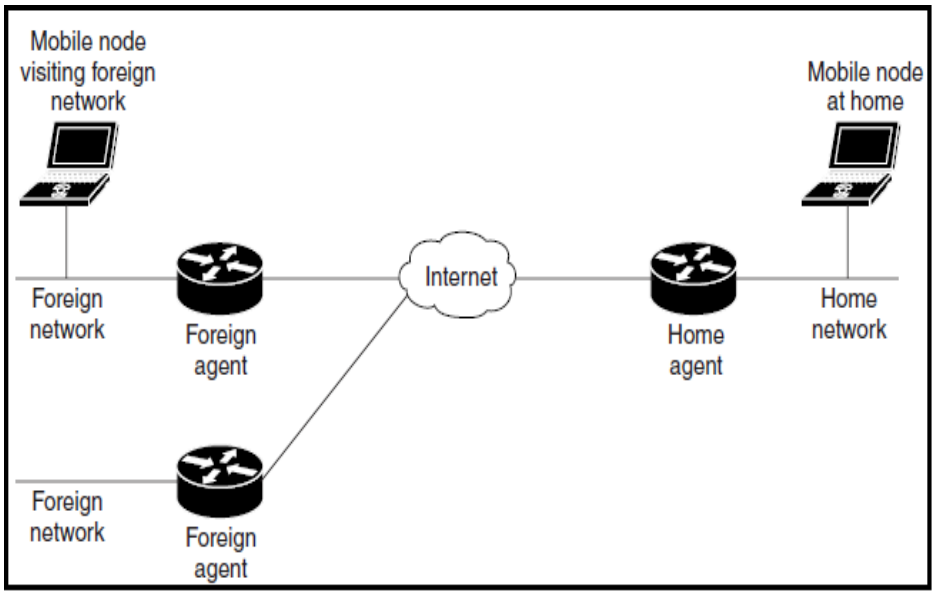


Figura 1. Componentes básicos de Mobile IP

Como se observa en la figura 1, Mobile IP introduce nuevos componentes o entidades:

**Mobile Node (MN):** básicamente es un host que tendrá la capacidad de cambiar su punto de acceso a una red, puede un PDA, Laptop o incluso un teléfono móvil con capacidad de acceder a redes IP.

**Home Agent (HA):** es un router de la red domestica en la que se encuentra un MN, este se encarga de mantener una asociación entre la dirección IP del MN y su *care-of address*, la cual es la localización actual del MN en una red visitada. El HA direcciona los paquetes por medio de encapsulación (túnel) hacia el MN mientras que este está fuera de su red domestica.

**Foreing Agent (FA):** es un router en una red foránea o visitada que asiste al MN en informar a su HA su actual *care-of-address*. El FA des-encapsula los paquetes que provienen del HA y los envía al MN. También actúa como el router por defecto para los paquetes generados por el MN mientras está conectado a la red foránea.

## 1.1. La necesidad de MoIP

Nuevos dispositivos y prácticas de negocios, tales como los PDA'S y los nuevos servicios de datos bajo las redes celulares, están sugiriendo la habilidad a los usuarios de moverse libremente mientras mantienen su conectividad. El requerimiento de conectividad para estos usuarios es muy diferente para los usuarios de líneas telefónicas o redes LAN cableadas. La solución debe estar entonces acomodada al reto del movimientos durante sesiones de datos o conversaciones por ejemplo.

Dado que las decisiones de enrutamiento están basadas en un prefijo de red de cada dirección IP, estas direcciones son escalables (pueden crecer). Cada nodo conectado a un enlace comparte el mismo prefijo de red. Si un nodo se mueve a otro enlace, el nuevo prefijo de red será diferente al que tenía. Consecuentemente, los paquetes IP no podrían ser debidamente direccionados y la información se perdería.

Como solución a este problema se podría pensar otro sistema de enrutamiento como lo es Host-specific routing, el cual solo utiliza el prefijo de host para direccionar los paquetes. Pero debido a la gran cantidad de host que existen en internet, esta no sería la mejor solución. DHCP también podría contemplarse como una solución, DHCP "alquila" una dirección IP que es asignada automáticamente por el servidor y configura automáticamente al host. Cuando el host deja la conexión, la dirección IP es reclamada por el servidor y queda disponible para otro usuario. Puesto que la asignación de la dirección IP es aleatoria, DHCP tampoco es la mejor solución para que un nodo móvil conserve su misma IP.

Mobile IP es escalable para internet ya que está basada en IP, por lo tanto, cualquier medio que use IP puede soportar Mobile IP. MoIP no cambia el prefijo de la IP del host, el cual es crítico para un apropiado enrutamiento de paquetes atreves de internet. Además, ciertas redes de servicios, tales como licencias de software y de acceso privilegiado, están basadas en direcciones IP. Entonces cambiar la dirección IP comprometería el funcionamiento de estas redes de servicio. Ciertas aplicaciones, tales como inicio de sesión remoto, impresión remota, y transferencia de archivos son ejemplos de aplicaciones donde es indeseable interrumpir la comunicación mientras un nodo móvil se mueve de una red a otra. En consecuencia, Mobile IP provee la solución para una continua conectividad.

## 1.2. ¿Cómo trabaja MoIP?

Mobile IP incluye tres fases principales, estas son:

- Descubrimiento y aviso del agente
- Registro
- Routing

Estas fases serán descritas en los capítulos siguientes.

## 2. DESCUBRIMIENTO Y AVISO DEL AGENTE

El descubrimiento y aviso del agéntele permite al nodo móvil:

- Determinar si está conectado a su red local o domestica, o si está conectado a un enlace foráneo (visitando otra red).
- Detectar si el nodo móvil ha cambiado su posición respecto a su punto de enlace.
- Obtener la CoA (Care-of Address) cuando haya cambiado su punto de enlace.

Durante la fase de descubrimiento del agente, los HA's y FA's advierten su presencia en su punto de enlace mediante el envío de múltiples emisiones (multicating ó broadcasting) llamadas *agent advertisements*. Los MN's escuchan estos anuncios y determinan o descubren si se encuentran en la red familiar o en la red foránea. En lugar de esperar los anuncios de los agentes, los MN's pueden enviar una solicitud de agente (*agent solicitation).* Esta solicitud obliga a cualquiera de los agentes a enviar los *agent advertisements.*

MoIP utiliza como método de descubrimiento del agente el protocolo ICMP (*Internet Control Message Protocol),* a continuación un breve repaso de este protocolo.

Antes que un host pueda empezar el envió de paquetes mas allá de su subred, primero debe descubrir la dirección de al menos un router de su red local, comúnmente esto es realizado por la lectura de una o más direcciones de Routers desde un archivo de configuración, por ejemplo, cuando el adaptador de red inalámbrica de un host móvil comienza la búsqueda de alguna red disponible, Otro método para descubrir la dirección de un router seria escuchar el protocolo de routing que usa dicho router, pero ¿qué sucede si estos métodos no proporcionan la capacidad de actualizarse automáticamente?, seguramente se generarían muchos problemas para administrar la red.

Los mensajes de ICMP son llamados "Router Advertisements" y "Router Solicitations", estos podrían considerarse como advertencias que hacen los Routers para avisar su ubicación y disponibilidad. Cada router emite periódicamente cada uno de estos mensajes anunciando la dirección IP de cada una de sus interfaces. Los hosts reconocen la dirección de sus Routers vecinos simplemente escuchando estas emisiones. Los mensajes para descubrir los router o agentes no constituyen en si un protocolo, estos permiten a los host descubrir la existencia de Routers vecinos mas no decide cual router es la mejor opción, esto se elige por la respuesta que proviene del router, la cual es re direccionada al host por intermediación del protocolo ICMP, un "Router Advertisement" incluye un nivel de preferencia para cada respuesta de las direcciones de un router. Esto representa una ventaja para el administrador de red ya que puede seleccionar o discriminar el uso de determinados Routers como router predeterminado. Los mensajes también cuentan con un campo de

“Lifetime” el cual especifica el tiempo máximo que una dirección advertida por un router tiene para ser considerada como válida por un host.

2.1 Agent advertisements

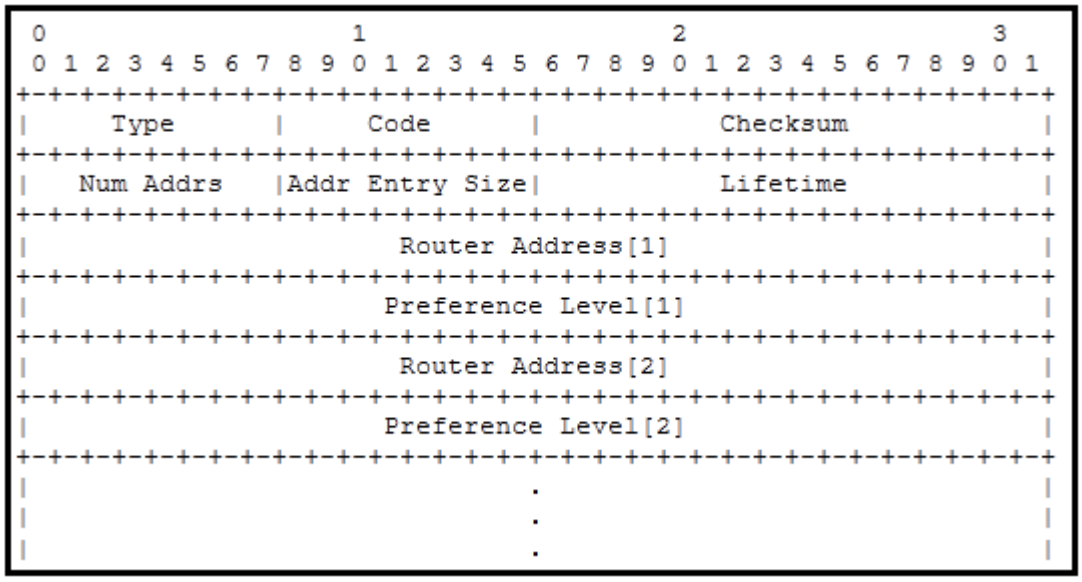


Figura 2. Mensaje ICMP Agent Advertisement

**Cabecera IP**

- Source Address: es la dirección IP de la interfaz desde la cual se envía el mensaje.
- Destination Address: es la dirección de destino o la dirección de un host vecino.
- Time-to-Live: debe ser 1 si la dirección de destino es multicast, es caso contrario este campo no debe ser menor a 1.

**Cabecera ICMP**

- **Type** 9
- **Code** 0
- **Checksum:** es el complemento a uno a 16 bit del complemento a uno de la suma del mensaje ICMP, comenzando con el ICMP Type. Para computar el Checksum, este campo es fijado en cero.
- **Num address:** es el número de direcciones de Routers advertidas en el mensaje.

- **Addr Entry Size:** numero de información por cada dirección de Router, estas son palabras de 32 bits y es fijado en 2.
- **Lifetime:** el número máximo de segundos que las direcciones de Router pueden ser consideradas validas.
- **Router address [1], i=1.Num Addrs:** Es la dirección IP de la interfaz del Router que envía el mensaje.
- **Preference Level[i], i=1... Num Addrs:** es la preferencia de cada dirección de Router para ser determinada la dirección por defecto con relación a las otras direcciones en la misma subred.

2.2Especificaciones de ICMP en los Agentes de movilidad (HA'S - FA'S)

Un Router que implemente el protocolo ICMP como mecanismo de detección de agentes debe permitir que ciertas variables sean configuradas por el administrador del sistema, aunque en muchos casos los valores por defectos no necesitan ser modificados.

**Para cada interfaz de Multicalst:**

**Advertisement Address:** dirección IP de destino que será usada para el envió de los Router advertisements (Multicast), la única dirección permitida para Multicast es 224.0.0.1, o también la dirección de Broadcast 255.255.255.255. Por defecto la dirección es 224.0.0.1, en caso que el router soporte IP multicast, sino, la dirección será 255.255.255.255.

**Max Advertisement Interval:** Es el máximo tiempo permitido entre cada envío de Router Advertisements desde una interfaz, en segundos. Este no debe ser menor de 4 segundos y no mayor de 1800 segundos.

Por defecto: 600 segundos.

**Min Advertisement Interval:** Es el mínimo tiempo permitido entre cada envió de Router Advertisements desde una interfaz, en segundos. Este no debe ser menor de 3 segundos y no mayor a Max Advertisement Interval.
Por defecto: 0.75*Max Advertisement Interval.

**Advertisement Lifetime:** valor a ser fijado en el campo de Lifetime de los Router Advertisements enviados desde la interfaz. No debe ser menor que Max Advertisement Interval y no mayor que 9000 segundos.
Por defecto: 3* Max Advertisement Interval.

**Para cada dirección IP de los Routers en sus interfaces de Multicast:**
**Advertise:** es una bandera (Flag) que indica si las direcciones son o no advertidas.
Por defecto: TRUE.

**Preference Level:** es la preferencia de una dirección como dirección de Router por defecto, esto se mide con respecto con las otras direcciones en la misma Subred. Este es un campo de 32 bits, con señalización, entre mayor es el valor, significa más preferencia, el valor mínimo (80000000 Hex) es usado para indicar que esta dirección no será usada como dirección por defecto por ningún Host vecino.
Por defecto: 0.

Se sugiere que cuando el nivel de preferencia de alguna dirección no ha sido explícitamente configurada, un Router puede configurarla de acuerdo a la métrica de los Routers, en lugar de fijarla a cero. Por tanto, un Router con la mejor métrica podría advertir un mayor nivel de preferencia para su dirección.

### 2.2.1 Validación de los mensajes por los Routers

Un Router debe descartar silenciosamente cualquier *Router solicitation* que no satisfaga los siguientes controles de validación:

- La dirección IP fuente es 0 ó o la dirección de un vecino (en caso de que la dirección sea igual a alguna de los Routers).
- El Checksum ICMP es válido.
- El código ICMP sea 0.
- La longitud del mensaje ICMP sea 8 o más octetos (derivado de la longitud de la cabecera IP).

El campo “Reserved” del mensaje ICMP y los octetos siguientes del octavo serán ignorados.

Una solicitud que pasa el control de validación es llamada “valid solicitation”.

2.3 Especificaciones en lo Nodos móviles (MN’S)

Cada Nodo Móvil deberá implementar el uso *Agent Solicitations* o R*outer Solicitations*, estas solicitudes deben ser enviadas solo en ausencia de *agent advertisements* o cuando una *care-of address* no ha sido determinada por el protocolo de la capa de enlace. El formato del mensaje de los *agent solicitations* usa los mismos mecanismos que los *agents advertisements***.**

**Agent solicitations**

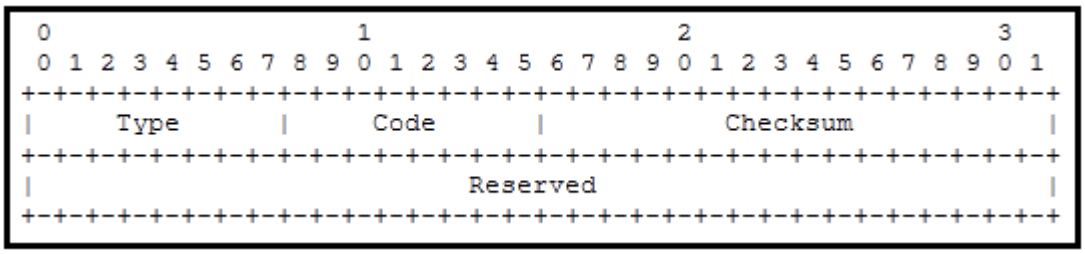

Figura 3.Mensaje ICMP Agent Solicitation

**Cabecera IP**

- Source Address: es la dirección IP de la interfaz desde la cual se envía el mensaje.
- Destination Address: dirección de solicitud configurada.
- Time-to-Live: debe ser 1 si la dirección de destino es multicast, es caso contrario este campo no debe ser menor a 1.

**Cabecera ICMP**

- **Type** 10
- **Code** 0
- **Checksum:** es el complemento a uno a 16 bit del complemento a uno de la suma del mensaje ICMP, comenzando con el ICMP type. Para computar el checksum, este campo es fijado en cero.
- **Reserved:** se envía un 0, ignorado en la recepción.

### 2.3.1 Variables de configuración en los Hosts

Cada Host que implemente el protocolo ICMP como mecanismo de detección de agente debe ser configurado con las siguientes variables:
Para cada interfaz multicast

- Perform Router Discovery: una bandera que indica si se está ejecutando o no ICMP en el Host. Default: TRUE.

- Solicitation Address: Es la dirección IP de destino usada para enviar *Router Solicitations* desde la interfaz. La única dirección permitida para este propósito 224.0.0.2 o la dirección de Broadcast limitada 255.255.255.255.

- Router Address: una dirección IP del Router por defecto. Default: NONE

- Preference Level: indica el nivel de preferencia que tiene el Host para determinar su Router por defecto. Está codificado en 32 bits y su máximo valor es 80000000 Hex, Default: 0.

### 2.3.2 Validación de los mensajes

Un Host descarta cualquier *Agent Advertisement* que no satisfaga los siguientes controles de validación:

- Checksum ICMP sea válido.
- Código ICMP sea cero.
- ICMP Num Addrs sea mayor o igual a 1.
- El tamaño del ICMP Addr Entry es mayor o igual a 2.
- La longitud del mensaje ICMP es mayor o igual a 8 + (Num Addrs*Addr Entry Size*4) octetos.

Un *Agent Advertisement* que pase los controles de validación será llamado *"Valid Advertisement"*

2.4 Detección de movimiento

Este mecanismo le permite a los MN's detectar si se está moviendo de una red a otra, cuando el nodo móvil detecta que se ha movido, entra en la fase de registro, como mecanismo de detección de movimiento se presentan los siguientes:

- Algoritmo 1: este mecanismo se basa en el campo de *Lifetime* junto con la principal porción del mensaje ICMP del *Agent Advertisement.* Los MN's deben ser capaces de grabar el valor del L*ifetime* recibido en un *Agent Advertisement* hasta que este expire. Si el nodo móvil falla en recibir otro *Advertisement* de un mismo agente en el *Lifetime* especificado, el nodo asume que ha perdido comunicación con el agente.

Si el MN ha recibido previamente un *Agent Advertisement* cuyo Lifetime no ha expirado, el nodo intentara inmediatamente registrarse con dicho agente.

- Algoritmo 2: este segundo mecanismo uso prefijo de red, los prefijos son usados en algunos casos por los MN's para determinar si un *Agent Advertisement* fue recibida desde la subred en la que se encuentra actualmente. Si el prefijo varia, el nodo móvil asume que se ha movido. Si el nodo móvil está siendo servido por un agente foráneo, este método no debería usarse a menos que un nuevo agente incluya también prefijos de red en sus *Agent Advertisements*. Se debe escoger este método de detección solo cuando todos los agentes utilicen los prefijos de red.

# 3. FASE DE REGISTRO

Luego de recibir una *Care-Of Address*, los nodos móviles registran esta dirección con su HA a través de un intercambio de mensajes. El HA crea una tabla de vinculación o enlace de movilidad (Mobility Binding) que asigna la dirección IP de la red domestica del MN a su nueva dirección de enlace (Care-Of Address). El principal propósito de la fase de registro es crear, modificar o eliminar una ligadura de movilidad de un MN de su HA.

El HA sigue advirtiendo la dirección IP domestica del MN aunque este ya no se encuentre en ella, esto permite que todos los paquetes destinados a esta dirección IP sigan siendo atraídos. Cuando un dispositivo en internet, en este caso llamado “nodo correspondiente” (CN), envía paquetes al MN, los paquetes son direccionados de manera común hacia el HA, este los intercepta y los encapsula, luego los tuneliza hacia la dirección donde el MN se ha registrado, es decir, hacia la red foránea. Los FA’s reciben los paquetes y los des-encapsulan nuevamente hacia el MN.

Si un nodo móvil está enviando solicitudes de registro a través de un FA, los agentes foráneos mantienen la pista de los MN visitantes manteniendo una lista de visitantes. Entonces los FA’s re-direccionan las solicitudes de registro directamente hacia el HA sin necesidad de tunelizar los paquetes. De esta manera, los FA’s sirven de Router para todos los paquetes enviados por el MN visitante.

Cuando un MN determina que debe reconectarse a su red domestica, se des-registra por medio del envió de solicitudes de de-registro al HA. Luego el HA recupera al MN.

Mobile IP define dos procedimientos de registro, uno por medio del FA el cual retrasmite el registro realizado por el MN hacia su HA, el otro consiste en un registro directo entre el MN y su HA. Las reglas que determinan cuál de estos procedimientos de registro se usan en determinadas circunstancias son:

- Si el nodo móvil se está registrando con una Care-of Address de un agente foráneo, el MN debe completar el registro a través del FA.
- Si un nodo móvil está usando una *Co-Located Care-Of Address*, el registro debe ser por medio del HA.

Ambos procedimientos de registro el intercambio de solicitudes de registro (*Registration Request*) y respuestas de registro (*Registration Reply*).

Si el registro se hace por medio de un FA, el procedimiento de registro requiere los siguientes mensajes:

a. El MN envía una solicitud de registro hacia el FA adecuado para empezar el registro.

b. El FA procesa la solicitud de registro y luego la retransmite hacia el HA del MN.

c. El HA envía una respuesta de registro al FA para conceder o denegar la solicitud.

d. El FA procesa la respuesta de registro y la retrasmite hacia el MN para informarle la disposición de su solicitud.

Si el MN se está registrando directamente con su HA:

a. El nodo móvil envía una solicitud de registro al HA.
b. El HA envía una respuesta de registro al MN concediendo o denegando su solicitud.

Los mensajes de registro usan el protocolo UDP como se estudiara a continuación.

3.1 Solicitudes de registro (Registration Request)

Un nodo móvil se registra con su HA por medio de mensajes de registro de tal manera que el HA pueda crear o modificar su tabla de movilidad (Mobility Binding) del MN. Como se mencionó, las solicitudes de registro deben ser retrasmitidas del FA al HA cuando el MN se registra con una Care-Of Address de un FA, o puede enviar las solicitudes directamente a su HA cuando se registra con una *Co-Located Care-Of Address*.

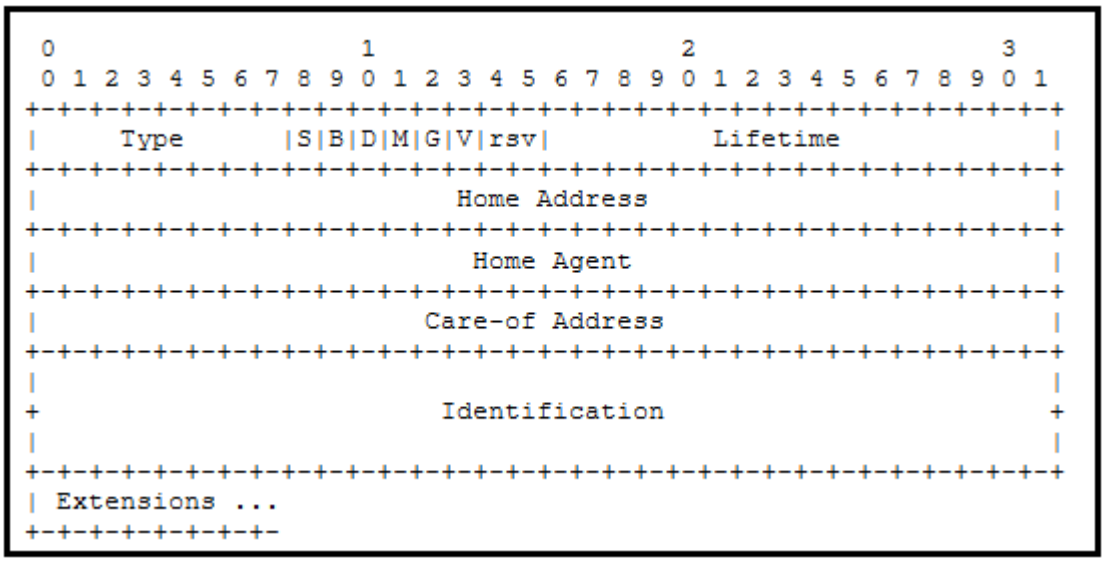


Figura 4. Mensaje de solicitud de registro

**Cabecera IP:**
Dirección Fuente (*Source Address)*: Típicamente es la dirección de la interfaz desde la cual se envía el mensaje.

Dirección de destino (*Destination Address*): típicamente la dirección del FA o del HA.

**Campo UDP:**
Puerto fuente (*Source Port*): puede variar

Puerto de destino (*Destination Port*): 434 mobileIP Agent.

**Campo Mobile IP**

Tipo (Type): 1 (solicitud de registro)

Enlaces simultáneos (S): si se fija el bit en “S”, significa que el MN está solicitando a su HA que mantenga el enlace prioritario de movilidad.

Datagramas Broadcast (B): Si se fija el bit en “B”, el MN está solicitando a su HA que tunelice cualquier datagrama Broadcast que reciba.

Des-encapsulación por MN (D): si se fija el bit en “D”, el nodo móvil se encargara de des-encapsular los paquetes que se envían a su Care-of Address.

Encapsulación mínima (M): Si se fija el bit en “M”, el MN solicita al HA que use una encapsulación mínima para los datagrama tunelizados hacia el nodo móvil.

Encapsulación GRE (G): Si el bit se fija en “G”, el MN solicita al HA que utilice encapsulación GRE para los datagramas.

Compresión Van Jacobson (V): si se fija el bit en “V”, el MN a su agente de movilidad que utilice la compresión Van Jacobson.

RSV: bit reservado enviado como cero.

Lifetime: el número de segundos faltantes antes que el registro se considere expirado. Un valor de cero indica que es una solicitud de de-registro. Un valor de 0xFFFF indica un Lifetime infinito.

Dirección domestica (Home Address): Dirección del MN.

Home Agent: dirección IP del HA de un MN.
Care-Of Address: dirección IP del final del túnel.

Identificación: Un numero de 64 bits construido por el nodo móvil, usado para comparar una solicitud de registro con una respuesta de registro con el fin de protegerlo contra mensajes de registro repetidos.

Extensiones: campo fijado para agregar extensiones a los mensajes de solicitud de registro.

3.2 Respuesta de registro (Registration Reply)

Las respuesta de registro son enviadas por los agentes de movilidad hacia los MN’s que han realizado una solicitud de registro. Si un nodo móvil está solicitando un servicio a un FA, ente agente foráneo recibirá una respuesta dese el HA y luego la retrasmite al MN. el mensaje de respuesta contiene la información suficiente para avisar al nodo móvil acerca del estado de su solicitud, junto con el Lifetime otorgado por el HA, el cual puede ser menor que el Lifetime de la solicitud inicial.

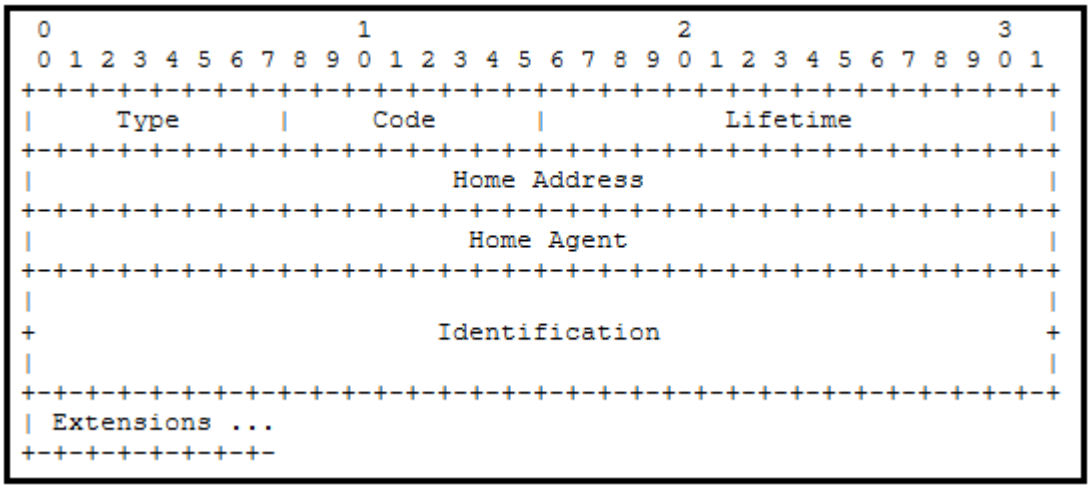


Figura 5. Mensaje de respuesta de registro.

**Cabecera IP:**

Dirección fuente (Source Address): típicamente es copia desde la dirección de destino de la solicitud de registro a la cual el agente está respondiendo.

Dirección de destino (Destination Address): copiada de la dirección fuente de la solicitud de registro a la cual el agente está respondiendo.

**Campo UDP:**

Puerto fuente: puede variar.

Puerto de destino: copiado del puerto fuente de la correspondiente solicitud de registro.

**Campo Mobile IP**

Type: 3 (Respuesta de registro).

Code: es un valor que indica el resultado de la solicitud de registro.

Lifetime: el campo “Code” indica que la solicitud de registro fue aceptada, el Lifetime es fijado como el número de segundos que el registro se considera expirado. Un valor de cero indica que el MN se ha des-registrado. Un valor de 0xFFFF indica un Lifetime infinito. Si por el contrario, la solicitud de registro es denegada, el valor del Lifetime no es especificado y debe ser ignorado en la recepción.

Home Address: Dirección IP del MN.

Home Agent: dirección IP del HA del MN.

Identification: Un numero de 64 bits construido por el nodo móvil, usado para comparar una solicitud de registro con una respuesta de registro con el fin de protegerlo contra mensajes de registro repetidos.

Extensions: campo fijado para agregar extensiones a los mensajes de respuesta de registro.

# 4. ROUTING

La fase de Routing describe como los nodos móviles, Home Agents y Foreing Agents cooperan para enrutar los paquetes hacia o desde los nodos móviles que están conectados a una red foránea. Los MN's informan a sus HA's su actual ubicación por medio de la fase de registro. Dado que la principal función de la capa de red es el enrutamiento, el mayor reto de Mobile IP es la de enrutar paquetes a Hosts que se están moviendo y cambiando su punto de enlace.

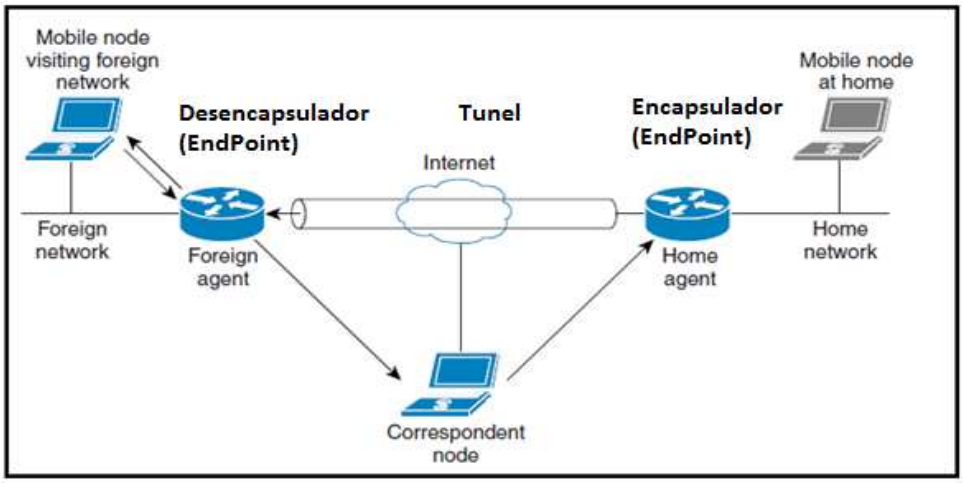


Figura 6. Tunneling

Mobile IP soluciona el inconveniente de enrutar los paquetes usando la técnica de "Tunneling" basándose en dos tipos de encapsulación:

## 4.1 Encapsulación IP-In-IP

La encapsulación es un método propuesto para alterar la manera en que normalmente los paquetes IP son direccionados por medio de un intermediario. Una vez el paquete es encapsulado, este llega a otro intermediario donde es des-encapsulado, recuperando el paquete original, el cual es finalmente entregado a su destinatario. El proceso de encapsulación y des-encapsulación es llamado "Tunneling", y los intermediarios (encapsulador y des-encapsulador) son llamados "Endpoints" del túnel (Figura #)

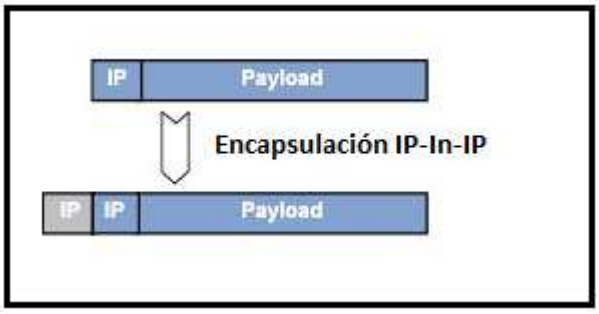

Figura 7. Encapsulación IP-In-IP

Para encapsular un paquete con encapsulación IP-In-IP, una cabecera IP externa debe ser insertada antes de la cabecera IP del paquete original. La cabecera IP externa contiene la dirección fuente y de destino de los "Endpoints" del túnel, mientras que la cabecera interna contiene la dirección fuente y de destino del paquete original, la cabecera interna no es modificada, solo se modifica su TTL (Time to life).

4.2 Campos de la cabecera IP externa

**Versión:** 4 (IPv4)

- **IHL**: (Internet Header Length) es la longitud de la cabecera IP externa medida en palabras de 32 bits.

- **TOS:** (Type of Service), es copiado de la cabecera IP interna (original).

- **Total Length**: longitud del paquete completo, incluyendo la cabecera externa e interna.

- **Identification, Flags, Fragment Offset**: este campo se copia de la cabecera IP interna.

- **TTL (Time to Life)**: se fija al valor apropiado para el envío del paquete encapsulado hasta el "Endpoint" del túnel.

**Protocol:** 4.

- **Checksum de cabecera**: Checksum de la cabecera externa.

- **Dirección fuente (Source Address)**: dirección IP del encapsulador que esta al inicio del túnel.

- **Dirección de destino (Destination Address)**: dirección IP del des-encapsulador que esta al final del túnel.

# 5. SEGURIDAD PARA MOBILE IP

Mobile IP nos proporciona las siguientes directrices para el manejo de la seguridad entre sus componentes:

- La Comunicación entre en nodo móvil y el Home Agent debe ser Autenticada.
- La Comunicación entre el nodo móvil y el Foreing Agent maneja Autenticación Opcional.
- La Comunicación entre el Foreing Agent y el Home Agent maneja Autenticación Opcional.

## 5.1 Nodo Móvil – Home Agent

El proceso de registro en Mobile IP siempre resulta ser bastante vulnerable a ataques a su seguridad, porque este le informa al Home Agent donde debe hacer túnel para enviar los paquetes hacia un Nodo Móvil en movimiento. Un nodo ilegitimo puede enviar un requerimiento de registro falso a un Home Agent y causar que todos los paquetes sean dirigidos a través de un túnel a el nodo ilegitimo en vez del Nodo Móvil. Este tipo de ataque se conoce como *denial-of-service attack*, impide que el Nodo Móvil envíe y reciba cualquier paquete.

Con el fin de prevenir este método de ataque a la conexión, se implementa que todo mensaje de registro entre el MN y él HA, sea autenticado.

Todo el proceso de autenticación comienza cuando un Nodo Móvil envía requerimientos de registro. El Nodo Móvil añade una estampilla de tiempo, compara el resumen de mensajes y luego añade la extensión de autenticación (MHAE) para el requerimiento de registro. El Home Agent recibe el requerimiento, se asegura de que la estampilla de tiempo es válida, computa el resumen de mensajes usando la misma llave y compara los resultados de los resúmenes de mensajes. Si los resultados concuerdan, el requerimiento es autenticado exitosamente. Para dar respuesta al registro, el Home Agent agrega la estampilla de tiempo,

computa el resumen de mensajes, y añade la extensión de la autenticación (MHAE) para la respuesta de registro. El Nodo Móvil autentica la respuesta de registro una vez que ha llegado desde el Home Agent.

### 5.1.2 Nodo Móvil – Foreign Agent

Mobile IP no requiere que la comunicación entre el Nodo Móvil y el Foreign Agent sea autenticada, pero permite que la autenticación entre Mobile – Foreign (MFAE) sea completamente opcional. MFAE protege la comunicación entre MN y FA manteniendo una clave compartida entre ambos.

### 5.1.3 Foreign Agent – Home Agent

Mobile IP no requiere que la comunicación entre el Foreign Agent - Home Agent (FHAE) sea autenticada. Pero permite que la autenticación entre Foreign - Home (FHAE) sea completamente opcional.

### 5.1.4 Home Agent – Home Agent

La comunicación entre un Home Agent activo y un Home Agent que se encuentre en Stand by, es decir, una topología de redundancia HA, debe ser autenticada. El proceso de autenticación trabaja de la misma manera que como lo describimos para el “Nodo Móvil – Home Agent”.

# 6. SIMULACIÓN

Una vez explicados todos los niveles y componentes que componen el protocolo MoIPv4, es el momento de llevar a la práctica dichos conceptos y presentarlos de manera grafica. Para alcanzar este propósito se ha seleccionado como herramienta de trabajo **QUALNET** software, información más detallada de esta herramienta es presentada a continuación.

## 6.1 Acerca de QUALNET

Quanlet es un conjunto completo de herramientas para el modelado de grandes redes cableadas e inalámbricas. Utiliza simulación y emulación para predecir el comportamiento y rendimiento de las redes para mejorar su diseño, funcionamiento y gestión.

Qualnet permite a los usuarios:

- Diseñar modelos de simulación para nuevos protocolos.
- Optimizar los modelos nuevos y existentes.
- Diseño de grandes redes cableadas e inalámbricas.
- Analizar el rendimiento de la redes y realizar su análisis.

### Interfaz grafica (Qualnet GUI)

El Qualnet GUI tiene cuatro componentes: Architect, Analyzer, Packet Tracer, y File Editor.

•**Architect:** es usado para crear escenarios (en modo de diseño) y también para correr las simulaciones (en el modo visualizar).

•**Analyzer:** en este modo se analizan los resultados de las simulaciones..

•**Packet Tracer:** es usado para analizar los trazos de los paquetes obtenidos al correr la simulación.

•**File Editor:** es usado para editar los archivos de textos.

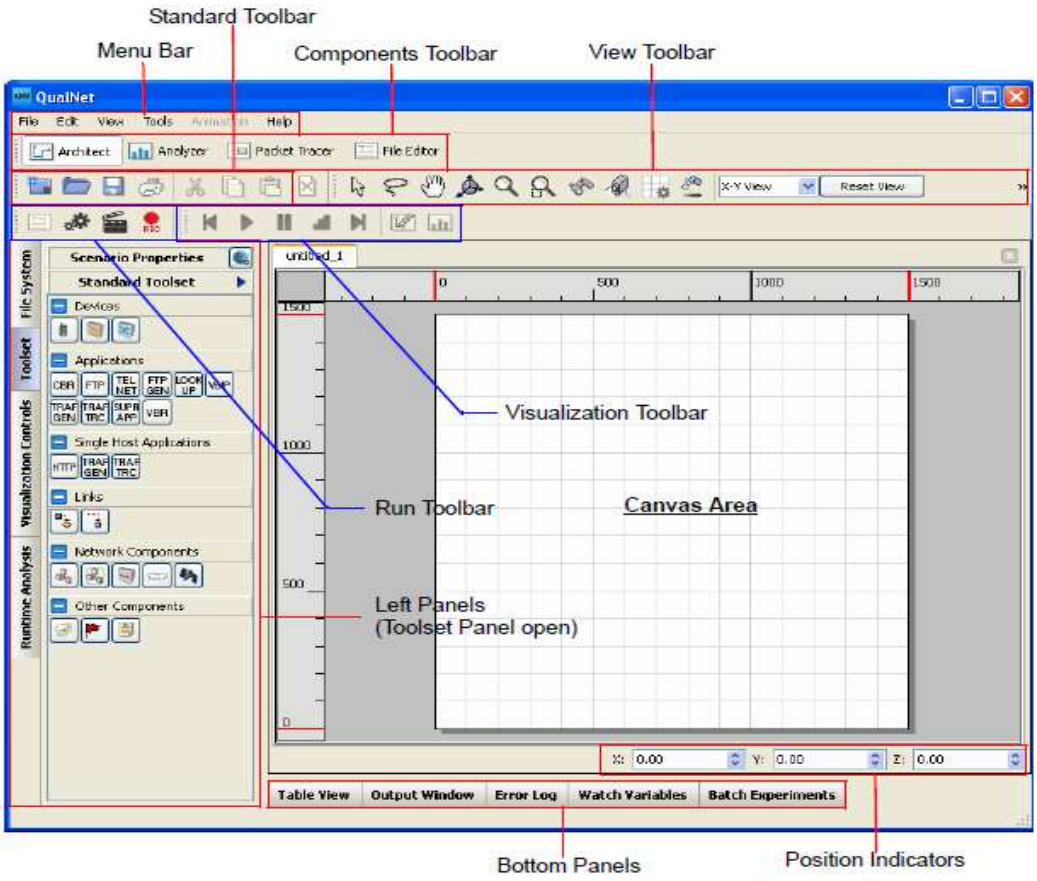


Figura 8. Intefaz grafica de Qualnet 5.0

6.2 Carasteristicas y asunsiones de mobile IPv4

**Caracteristicas implementadas**

- Care-of Address de FA's
- Ruteo de datagramas unicast

**Caracteristicas omitidas**

- Capacidad de enrutamiento a los nodos moviles.
- Uso de *Co-located care-of address*.
- Autenticacion.
- Redes virtuales
- Enrutamiento de datagramas broadcast y multicast

**Asunsiones y limitaciones**

- Mobile IP es soportado solo cuando esta corriendo OSPFv2 como protocolo de enrutamiento en los agentes de movilidad.
- Mobile IP es soportado solo cuando esta corriendo 802.11MAC como procolo MAC.
- Para correr Mobile IP, los nodos moviles deben estar configurados con el modelo de movilidad “FILE”.
- Una red foranea solo puede tener un Foreing Agent.
- Cualquier nodo Wireless no puede tener mas de una interfaz Wireless.

6.3 Escenario

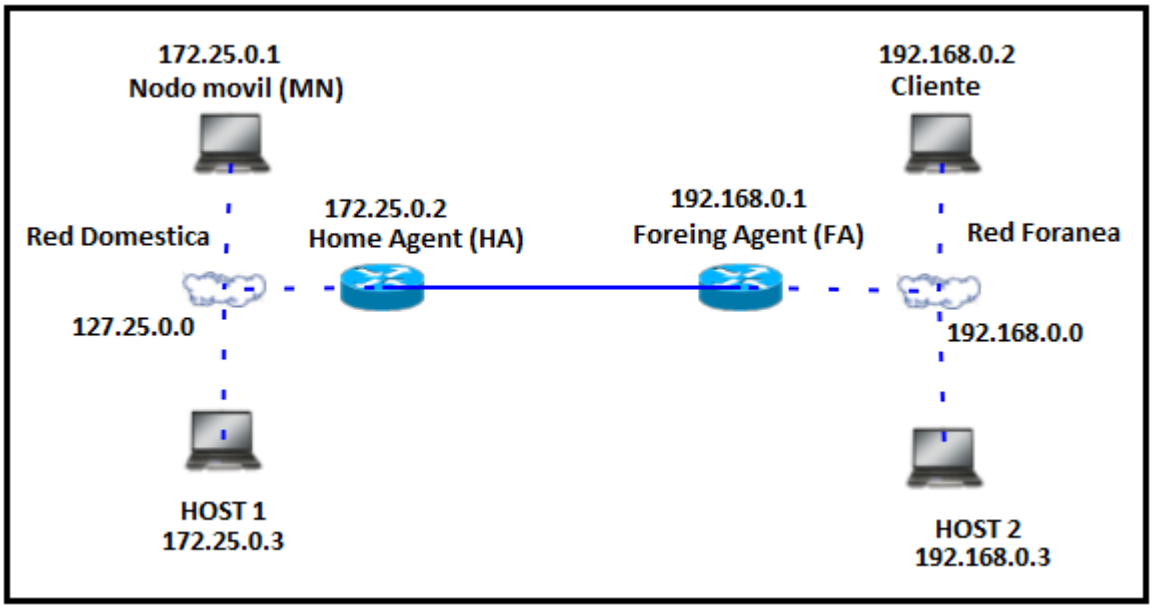


Figura 9. escenario Mobile IP

**6.3.1 Descripcion del escenario:**

- El escenario esta compuesto por dos redes, una red domestica y una foranea.
- La red domestica esta compuesta por el nodo movil, un Host cualquiera y un Home Agent.

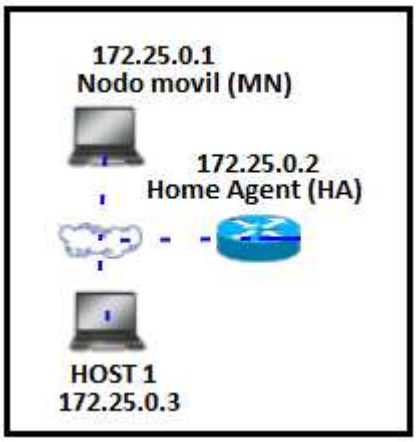


Figura 10. Red Domestica

- La red foranea esta compuesta por un cliente, un host cualquiera, y el Foreing agent.

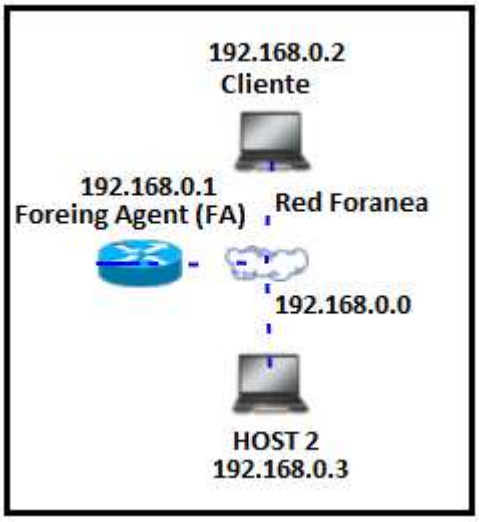


Figura 11. Red Foranea

- El nodo movil esta configurado para que se desplace de su posision hacia la cobertura de una red foranea.

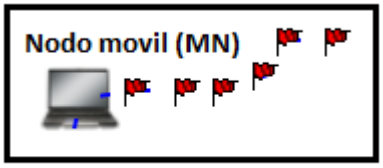


Figura 12. Desplazamiento del MN

- El nodo movil y el cliente mantendran una aplicacion CBR (Costant Bit Rate) que enviara una tasa de bit constante durante la simulacion.

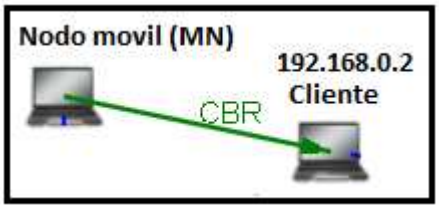


Figura 13. Aplicación entre el nodo movil y el cliente

- Un terreno urbano es usado para ubicar los nodos y trazar la ruta de movilidad del MN.

## 6.4 Configuracion del escenario en Quanlet 5.0

Para configurar el escenario anteriormente descrito, se debe seleccionar los respertivos componentes de red (Routers, Hosts, subredes, links), al igual que las aplicaciones. Para esto, se ubica cada componente en el "Toolset Panel" del GUI de Qualnet.

### 6.4.1 Configuracion de las subredes

Para agregar las subredes hay que ubicarse en "Network Components" del Toolset panel, seleccionamos el icono "Wireless Network" y lo arrastramos hasta el area de trabajo (Canvas Area).

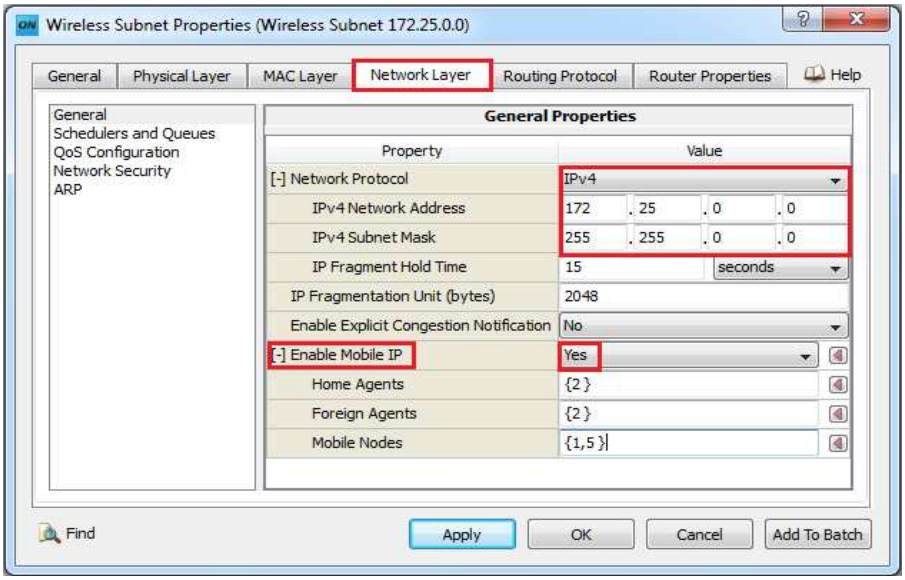


Figura 14. Configuración de red Wireless.

Una vez ubicados en el área de trabajo, configuramos las propiedades de la red haciendo doble click en el icono. Ubicamos la pestaña “Network Layer” y configuramos los siguientes parámetros:

Para la subred # 1:

- Network Protocol: se selecciona IPv4.
- Se establece la dirección IP [172.25.0.0], con máscara de subred [255.255.0.0].
- Habilitamos la opción “Enable Mobile IP” marcando la opción “Yes”.
- se rellenan los campos de Home Agent y Foreign Agent en 2 (nodo 2), mientras que en Mobile Nodes se rellenan con 1 y 5 (nodos 1 y 5).

De igual manera:

Para la subred # 2:

- Network Protocol: se selecciona IPv4.
- Se establece la dirección IP [192.168.0.0], con máscara de subred [255.255.255.0].
- Habilitamos la opción “Enable Mobile IP” marcando la opción “Yes”.
- se rellenan los campos de Home agent y Foreign Agent en 3 (nodo 3), mientras que en Mobile Nodes se rellenan con 4 y 6 (nodos 4 y 6).

En la pestaña MAC Layer, se selecciona “MAC Protocol” como 802.11.

### 6.4.2 Configuración de los agentes de movilidad (HA Y FA)

Para configurar ya sea él HA o el FA, abre el cuadro de propiedades y ubicamos la pestaña “Node Configuration”, luego la opción “Network Layer”.

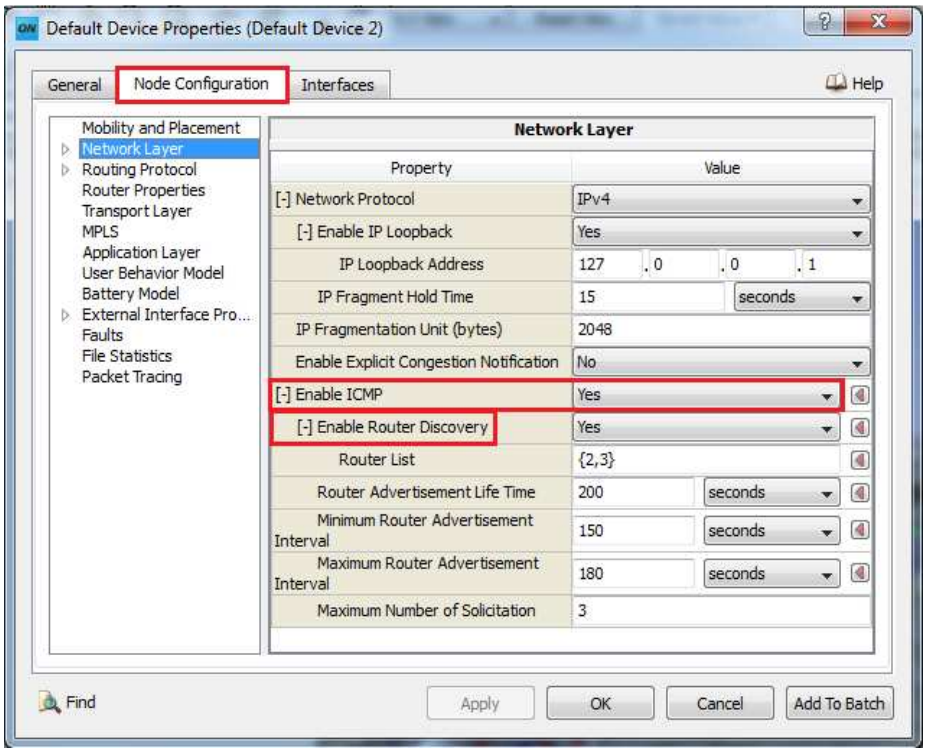


Figura 15. Configuración de ICMP en HA y FA

Aquí se configura lo siguiente:
Network Protocol : IPv4 (por defecto).

- Se habilita la opción “Enable ICMP” seleccionando “Yes”.
- Luego se expande la opción “Enable Router Discovery” y seleccionamos “Yes”
- Rellenamos la opción “Router List” con los valores 2 y 3, que son los nodos que actuaran con HA y FA, por lo tanto estos también serán los Routers ICMP.

Finalmente se completan los siguientes campos:

Router Advertisement Lifetime: 200s

Minimum Router Advertisement interval: 150s

Maximum Router Advertisement interval: 180

Maximum Number of Solicitations: 3

Ahora ubicamos la opción “Routing Protocol”

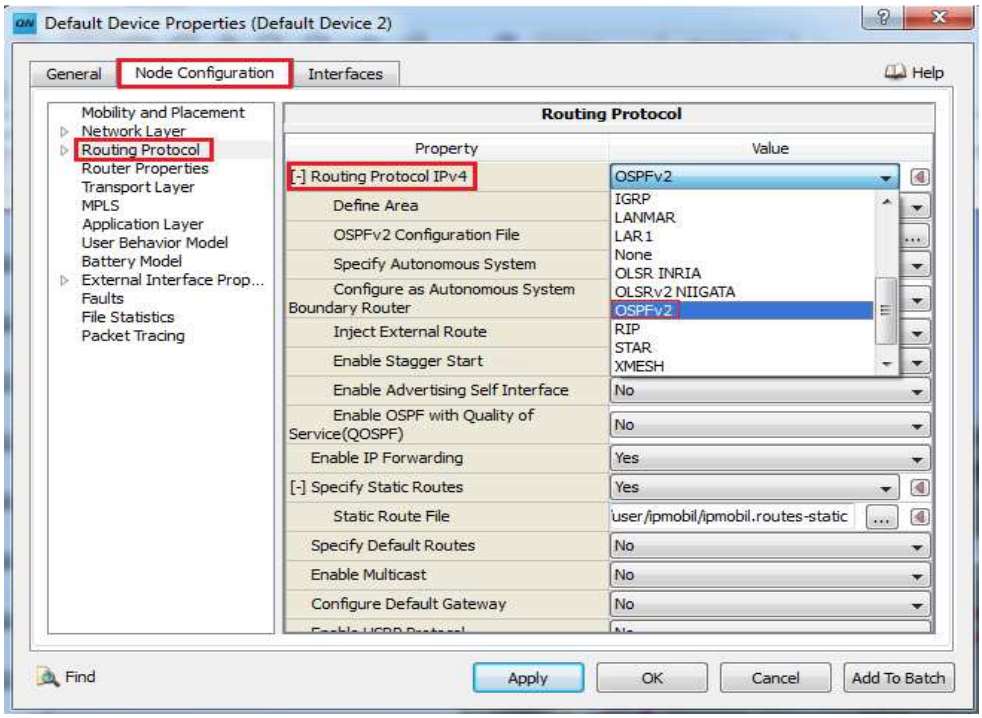


Figura 16. Configuración de protocolo de enrutamiento HA y FA

Seleccionamos la opción “OSPFv2” y guardamos los cambios.

### 6.4.3 Configuración de los nodos móviles (MN)

Abrimos el cuadro de propiedades de los nodos móviles y configuramos los siguientes parámetros:

Ubicamos “Node Configuration”, luego en la opción “Mobility and Placement”, en la casilla “Mobility Model” marcamos la opción “File”.

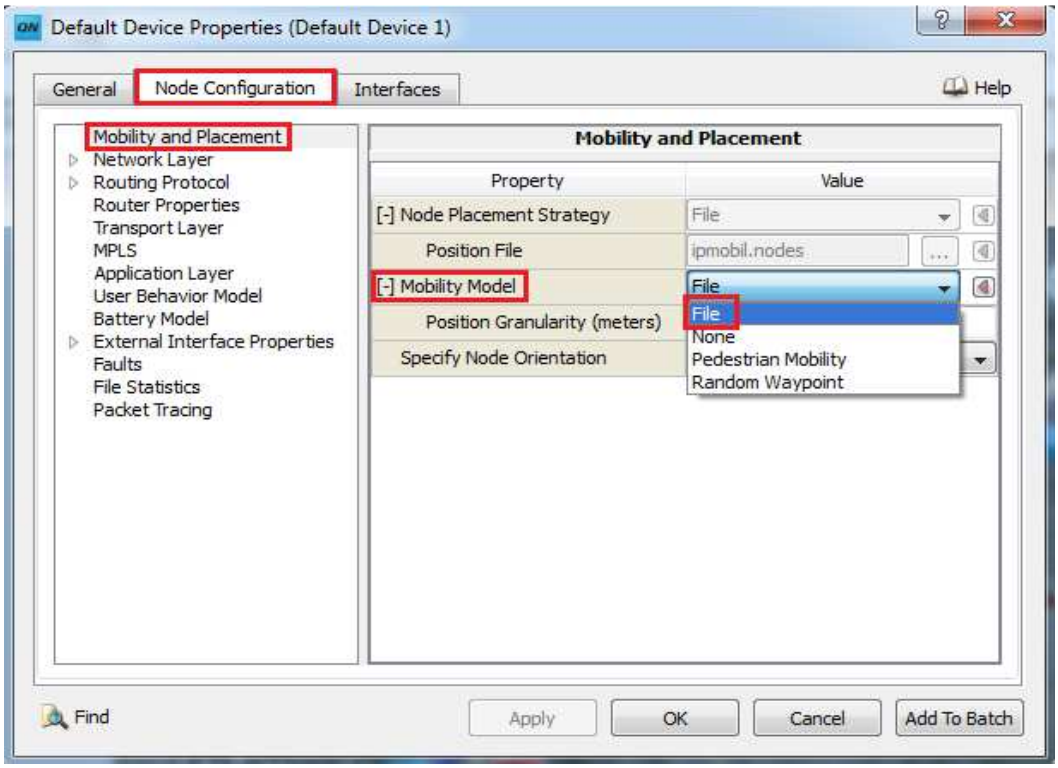


Figura 17. Configuración de Movilidad para los MN's.

Ahora nos dirigimos a la opción "Network Layer" y configuramos:

- "Enable ICMP": marcamos "Yes".
- "Enable Router Discovery": marcamos "Yes".
- "Router List": rellenamos con 2 y 3.
- Router Advertisement Lifetime: 15s
- Minimum Router Advertisement interval: 5s
- Máximum Router Advertisement interval: 10
- Máximum Number Of Solicitations: 3

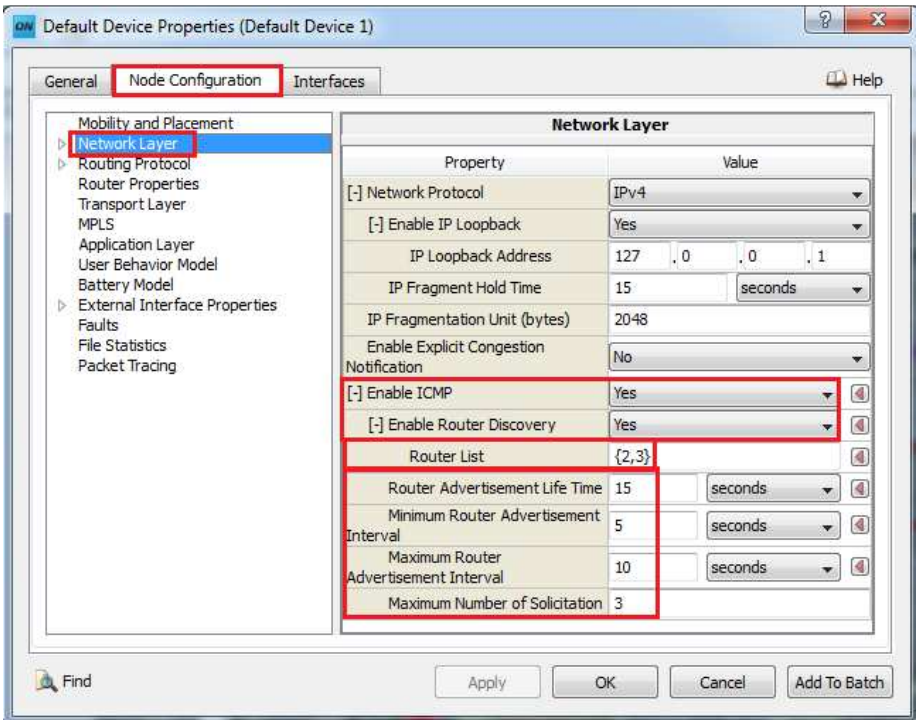


Figura 18. Configuración ICMP para los MN's.

Luego en la opción "Routing Protocol" seleccionamos "None".

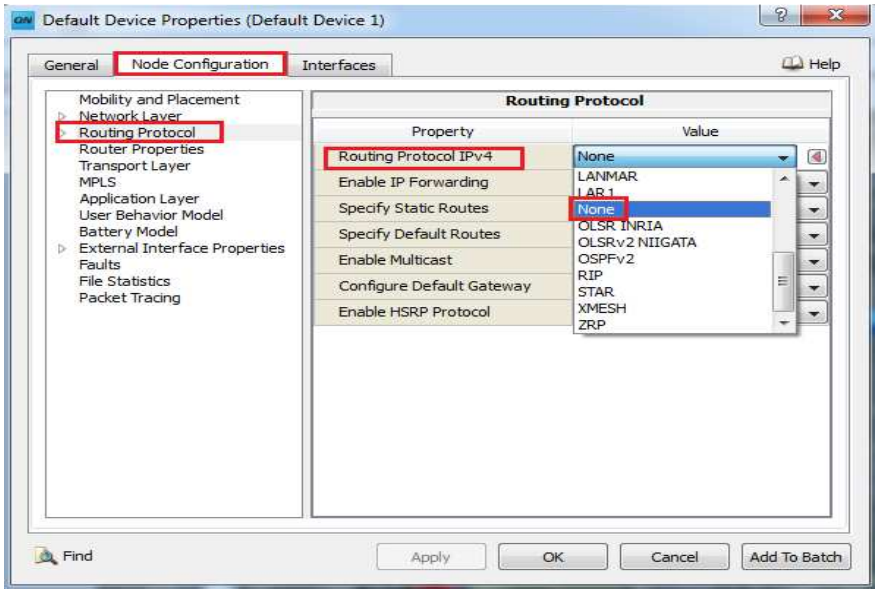


Figura 19. Configuración de protocolo de enrutamiento para los MN's.

### 6.4.4 Configuración de los enlaces “Link”

Para agregar los enlaces debemos ubicar el icono “link” en la sección de “Links” en el “Standard Toolset”.

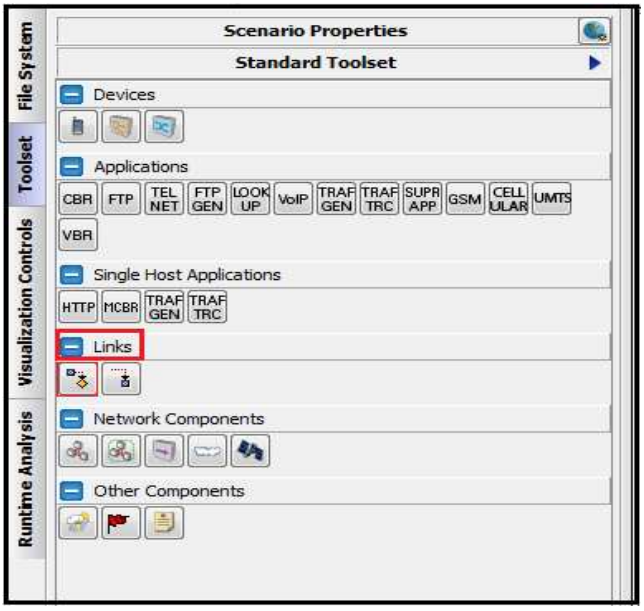


Figura 20. Ubicación del icono “Link”.

Para realizar un enlace se debe dar click en un nodo, manteniendo el click, arrastramos el cursor hasta seleccionar el otro nodo con el cual deseamos hacer el enlace. El enlace puede ser “Wireless”, cableado “Wired” y microondas “Microwave”.

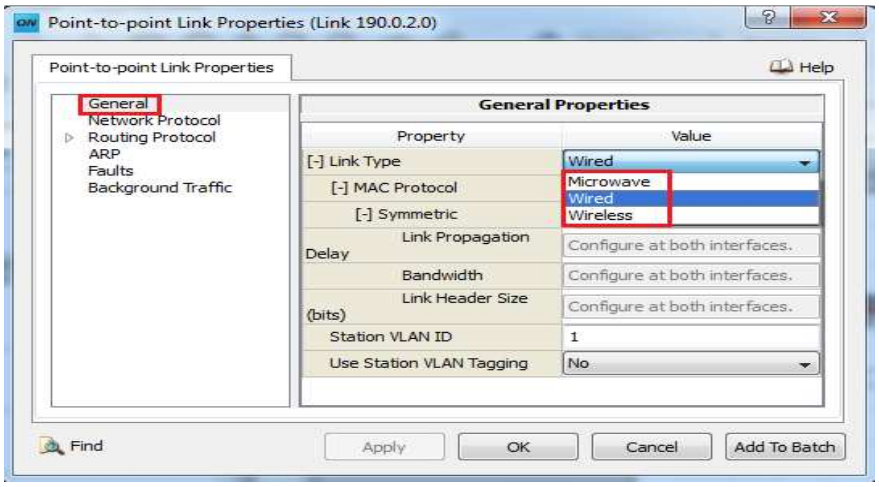


Figura 21. Propiedades de los Links.

### 6.4.5 Configuración de las aplicaciones

Para configurar las aplicaciones hay que dirigirse a la sección “Applications” en el “Estándar Toolset”. Aquí encontramos aplicaciones Cliente-Servidor y aplicaciones de Hosts (Single Host Applications).

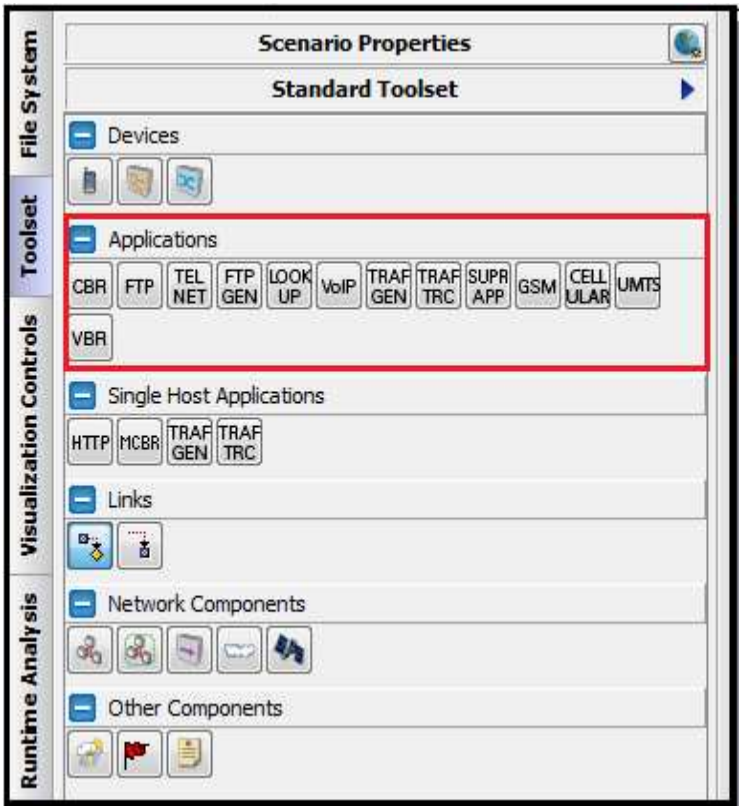


Figura 22. Aplicaciones.

Para esta simulación se escoge la aplicación “CBR” (Constant Bit Rate), esta aplicación correrá entre los nodos 1 y 4, entonces hacemos la unión de la aplicación dando click en el nodo 1 (servidor) y lo arrastramos hasta el nodo 4 (Cliente), luego configuramos las propiedades de la aplicación así:

Source: 1  destination: 4.

**Items to Send**: 0, **Item Size (Bytes):** 512, **Interval:** 0.01s, **Start Time**: 20, **End time**: 0s.

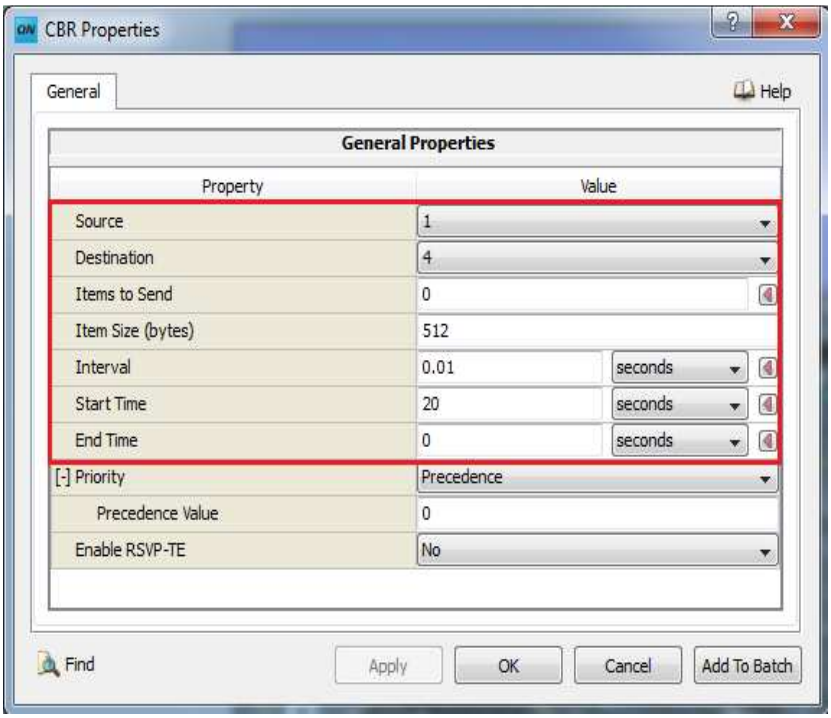


Figura 23. Configuración de aplicación CBR

Esta configuración permitirá que haya una transferencia constante de bits a partir de los 20s hasta que finalice la simulación.

6.5 Configurar las propiedades del escenario y las estadísticas

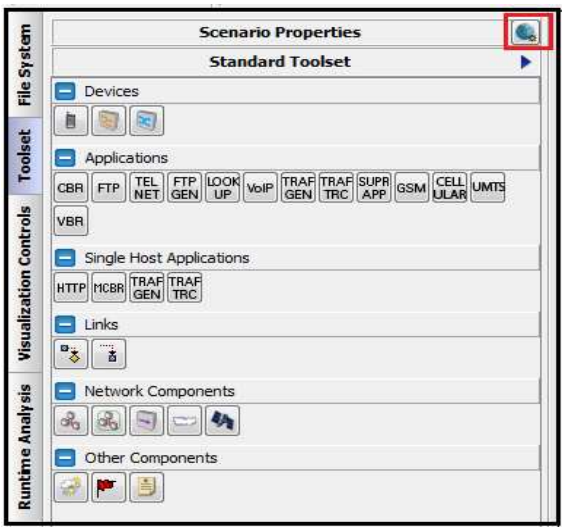


Figura 24. Ubicación de propiedades del escenario.

En la opción “General Settings” seleccionamos el tiempo de la simulación, en este caso es de 190 s. si se quiere agregar un fondo al area de trabajo se puede hacer en la opción “Scenario Background Image File”.

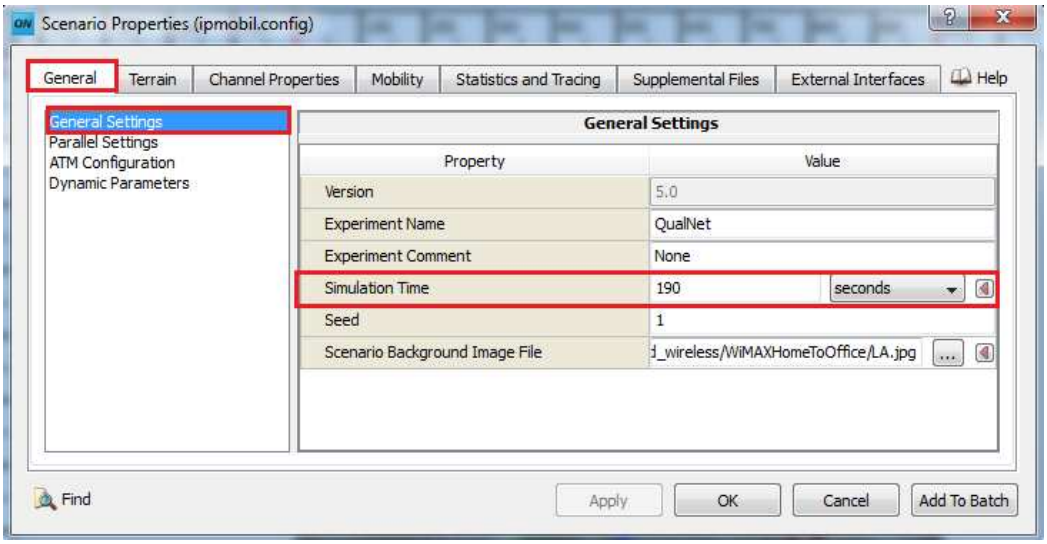


Figura 25. Propiedades generales del escenario.

En la opción “Statistics and Tracing”, además de las opciones que están marcadas, seleccionamos las opciones de Mobile IP e ICMP.

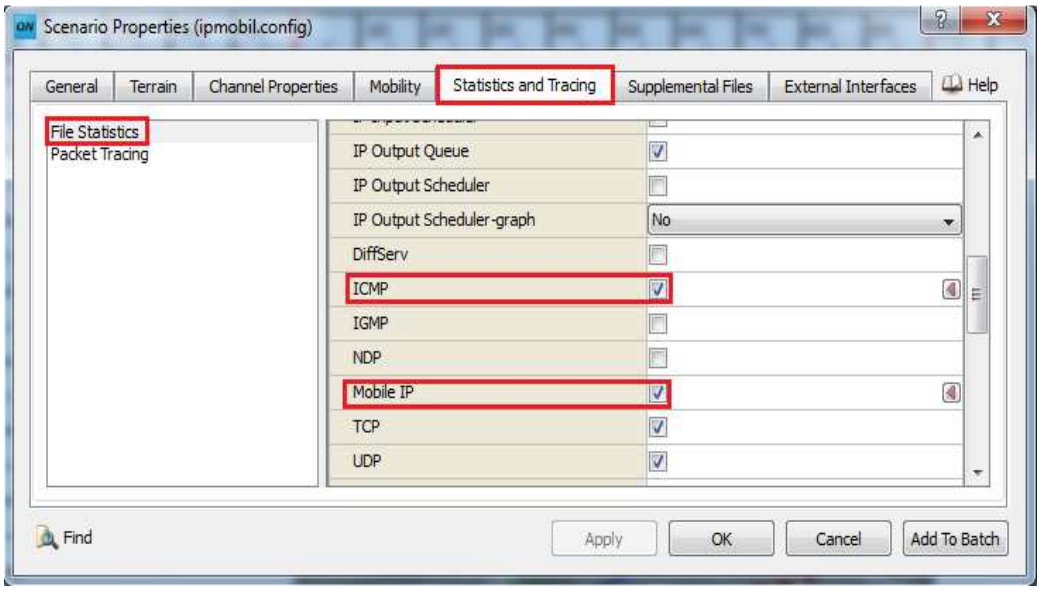


Figura 26. Configuración de estadísticas.

## 6.6 Corriendo la simulación

Después de haber realizado las configuraciones pertinentes el escenario está listo para su ejecución. Para ello ubicamos el icono “Run Simulation”  .

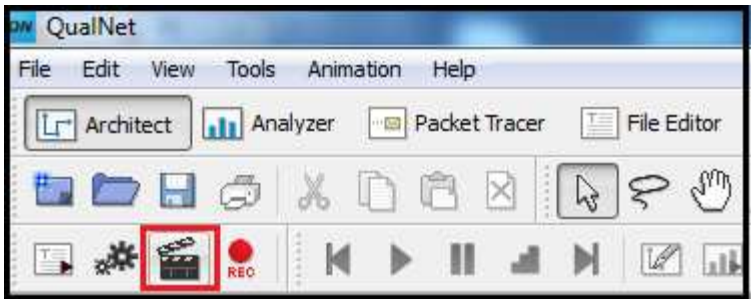


Figura 27. Icono “Run Simulation”.

Si todo sale bien, se activa la barra de visualización  , y damos click en play  .

Luego comenzaremos a observar la actividad de la simulación, aquí se puede apreciar la transferencia de datos, la comunicación entre los distintos nodos, incluso la propagación de la señal por parte de los nodos.

## 7. RESULTADOS Y ANÁLISIS

Dado que la simulación es animada (Dinámica), presentamos la etapa inicial de la simulación:

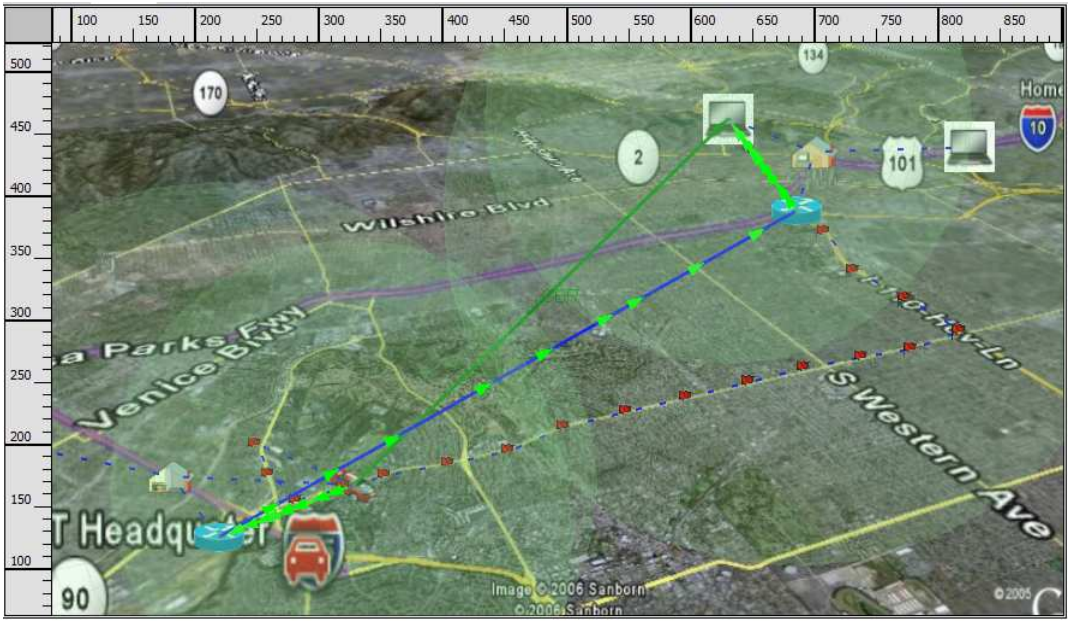


Figura 28. Transferencia de datos a través del HA

El escenario fue finalmente configurado para trabajar sobre un terreno urbano, la red domestica está en la parte inferior izquierda, un usuario de esta red se encuentra en su auto y desea desplazarse varia cuadra hasta su oficina (red foránea) mientras mantiene una aplicación CBR con un nodo en dicha red foránea, la trayectoria está marcada con las banderas (Figura #). Mientras el usuario se encuentra en el área de cobertura de su red domestica, la transferencia de datos se realiza de manera común a través de su Router por defecto (Home Agent), al mismo tiempo, el nodo móvil detecta que se está moviendo y empieza a enviar *Agent solicitations*, al igual que los agentes de movilidad envían *Agent Advertisements*.

Luego que el MN empieza a alejarse de su red domestica, empieza a entrar en la cobertura de una red foránea, si el FA le envía un *Agent Advertisement* el nodo móvil puede comenzar la etapa registro y hacer el Handover. A partir de este punto, el HA sede al FA la capacidad de enrutamiento de los paquetes hasta entregarlos a su destino (Figura 29).


Figura 29. Transferencia de datos a través del FA

7.1 Análisis de estadísticas

### 7.1.1 Estadísticas de la aplicación

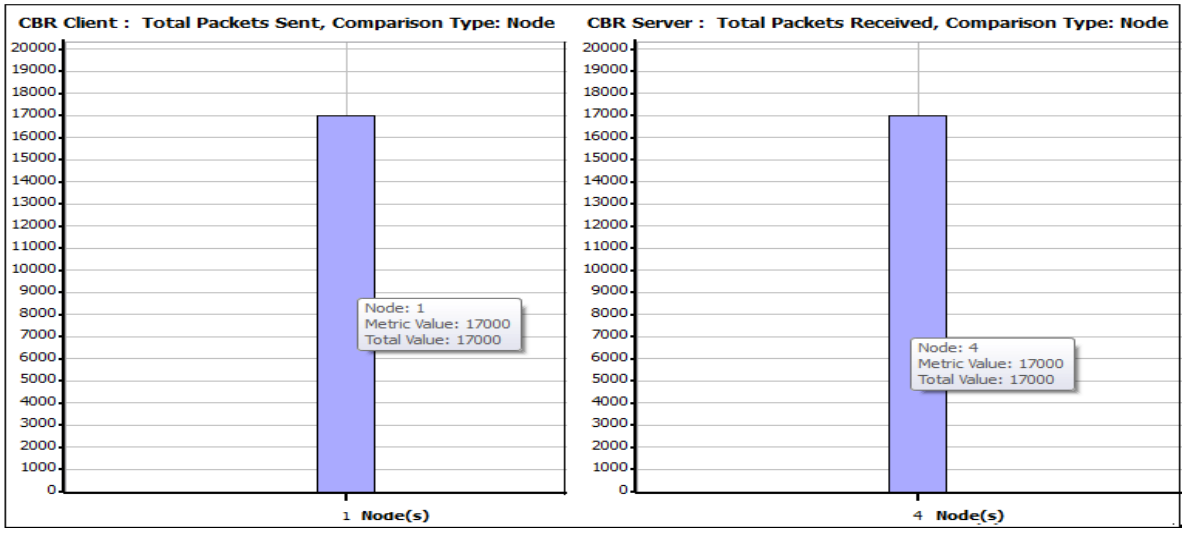


Figura 30. Paquetes enviados y recibidos Cliente-Servidor

Se puede observar que la cantidad de paquetes enviados es la misma que los recibidos, lo que quiere decir que la aplicación no tuvo pérdidas de paquetes a pesar que el MN cambio su punto de enlace.

Paquetes enviados: 17000

Paquetes recibidos: 17000

7.2 Estadísticas ICMP

### 7.2.1 Advertencias del agente (Agent Advertisements):

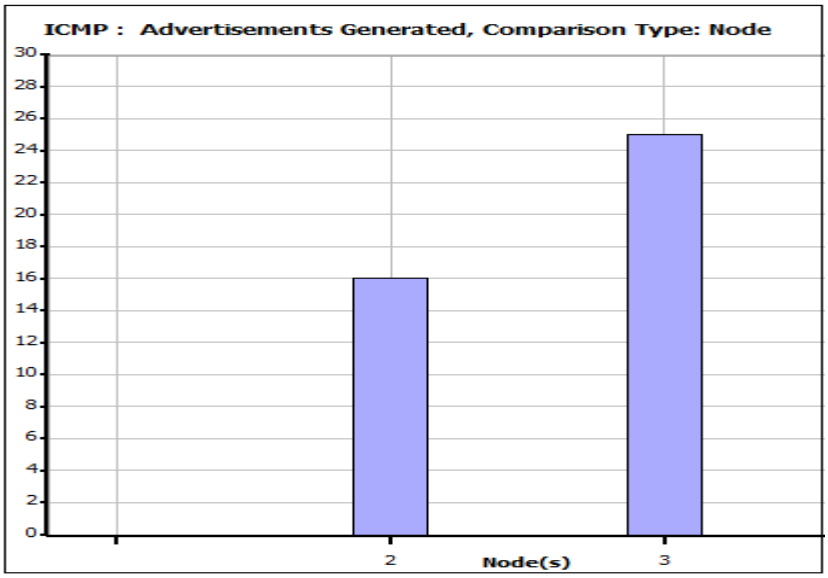


Figura 31. Agent Advertisements generadas

Se observa que los agentes de movilidad en función de Routers ICMP, generaron Agent Advertisements para indicar su disponibilidad. Note que la cantidad se advertencias emitidas por el HA (Nodo 2) es menor que la cantidad generada por el FA (nodo 3), esto se debe a que la configuración ICMP del FA se realizo de manera que pudiera encontrar de manera oportuna cualquier nodo móvil que lo visite.

Agent Advertisement por el HA: 16

Agent Advertisement por el HA: 25

### 7.2.2 Advertencias recibidas

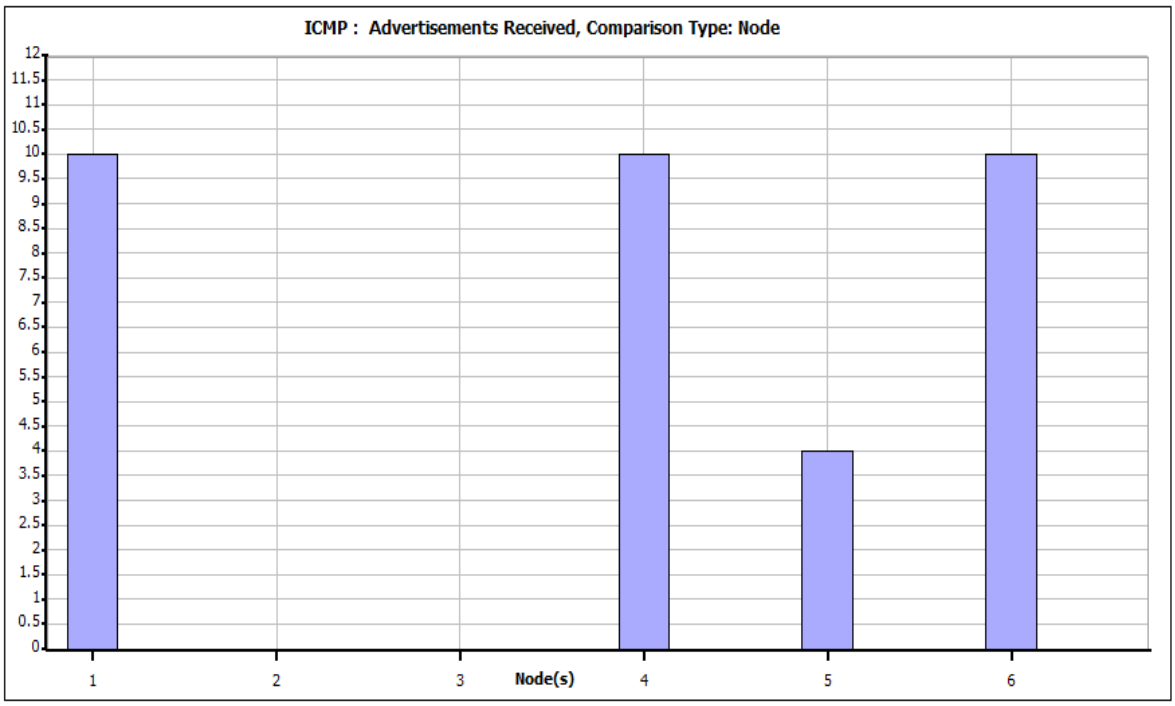


Figura 32. Advertencias recibidas

Las advertencias solo son recibidas por los nodos móviles. Aquí se observa la actividad de cada MN respecto a los agentes de movilidad. Los nodos 1,4 y 6 recibieron 10 advertencias, mientras que el nodo 5 recibió 4 advertencias. Note que el nodo que se está desplazando recibió una gran cantidad de advertencias por parte de los agente de movilidad, esto permite que el nodo móvil y los agentes puedan tomar las decisiones a tiempo en cuanto llevar a cabo el Handover.

### 7.2.3 Solicitudes de agente generadas (Agent Solicitations)

En ausencia de *Agent Advertisements*, los nodos tienen la capacidad de usar el protocolo ICMP para descubrir la presencia o ausencia de dichos agentes. Se observa que los nodos 1,4 y 6 generaron 3 solicitudes de agente, mientras que el nodo 5 genero 5 solicitudes. Note que ahora sucede lo contrario a los *Agents Advertisements*, los nodos que recibieron más advertencias tuvieron que generar menos solicitudes que aquellos que recibieron menos advertencias.

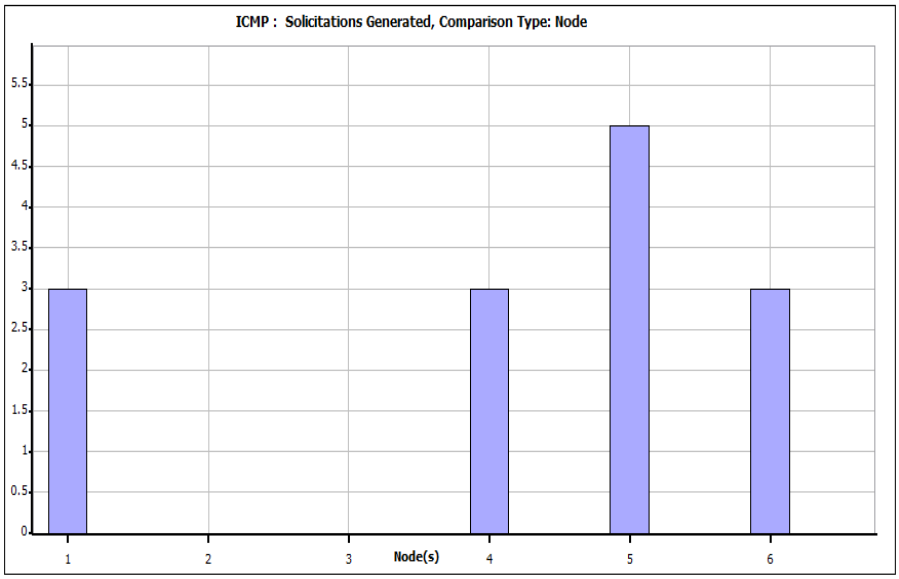


Figura 33. Solicitudes de agente generadas.

### 7.2.4 Solicitudes recibidas

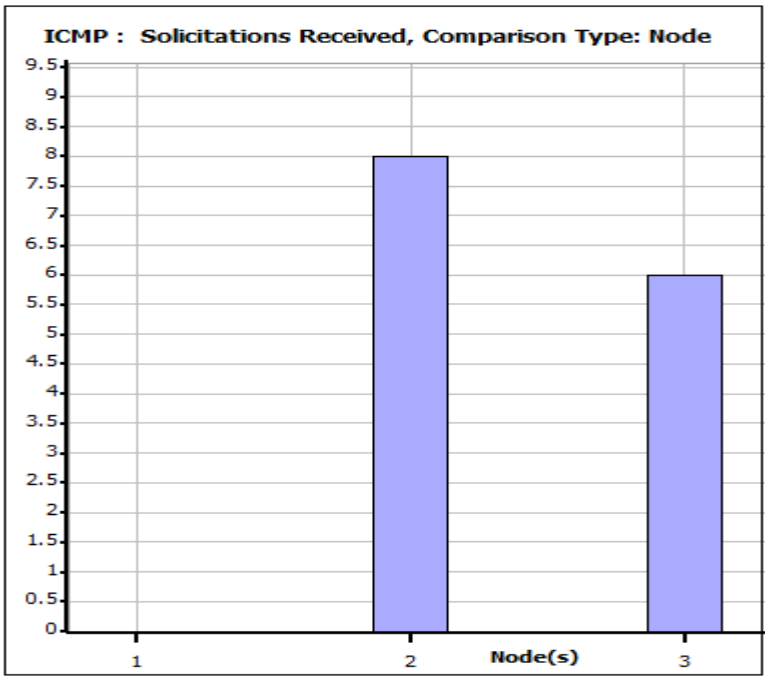


Figura 34. Solicitudes recibidas

Las solicitudes generadas por los nodos móviles fueron escuchadas por los agentes de movilidad. Se puede notar que el nodo 2 (Home Agent) recibió más solicitudes que el nodo 3 (Foreign Agent), debido a que él HA advierte menos seguido su presencia a los nodos móviles, por lo que estos inician una búsqueda permanente para encontrar un agente enviando así muchas solicitudes.

7.3 Estadísticas Mobile IP

### 7.3.1 Solicitudes de registro realizadas (Registration Request)

Luego de haber recibido y aceptado los *Agent Advertisements*, los MN's entran en la fase de registro y empiezan a enviar solicitudes de registro y registrar su nueva Care-Of Address. Aquí se observa la actividad de los nodos móviles, El nodo 1 solicitó 11 peticiones para registro, los nodos 4 y 6 solicitaron 10, y el nodo 5 generó 4 solicitudes. En total fueron 35 solicitudes generadas.

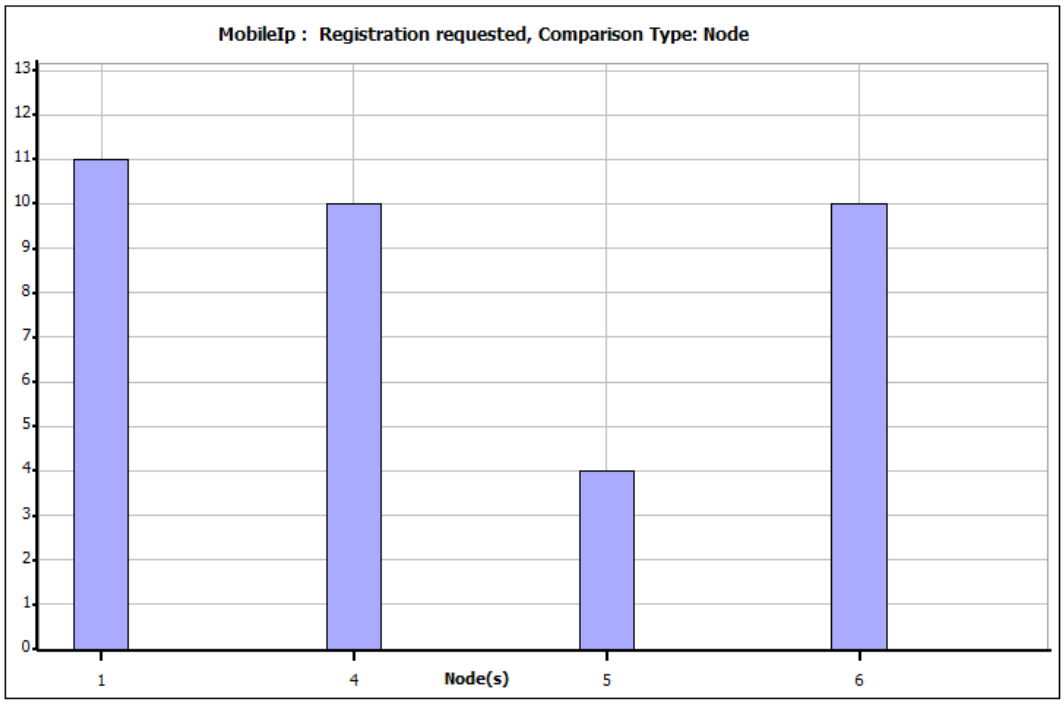


Figura 35. Solicitudes de registro realizadas

### 7.3.2Solicitudes de registro recibidas por los agentes de movilidad

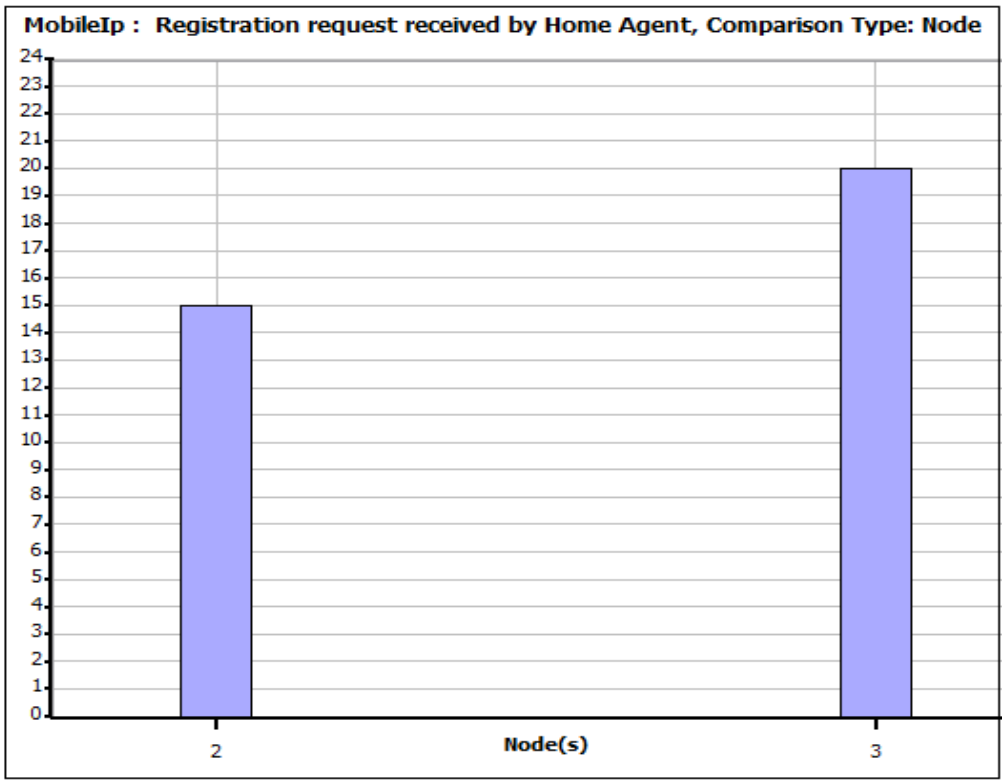


Figura 36. Solicitudes de registro recibidas en los agentes

Cada una de las solicitudes generadas fueron recibidas por los agentes de movilidad, en total los agentes recibieron 35 solicitudes entre ambos.

### 7.3.3Solicitudes de registro retransmitidas por el FA

Muestra la actividad del FA retransmitiendo las solicitudes recibidas. Estas solicitudes provienen de un nodo visitante que requiere registrarse con esta nueva red foránea, pero antes que esto ocurra, el FA debe transmitir esta petición al HA del nodo visitante. En total, el FA retransmitió 7 solicitudes de registro.

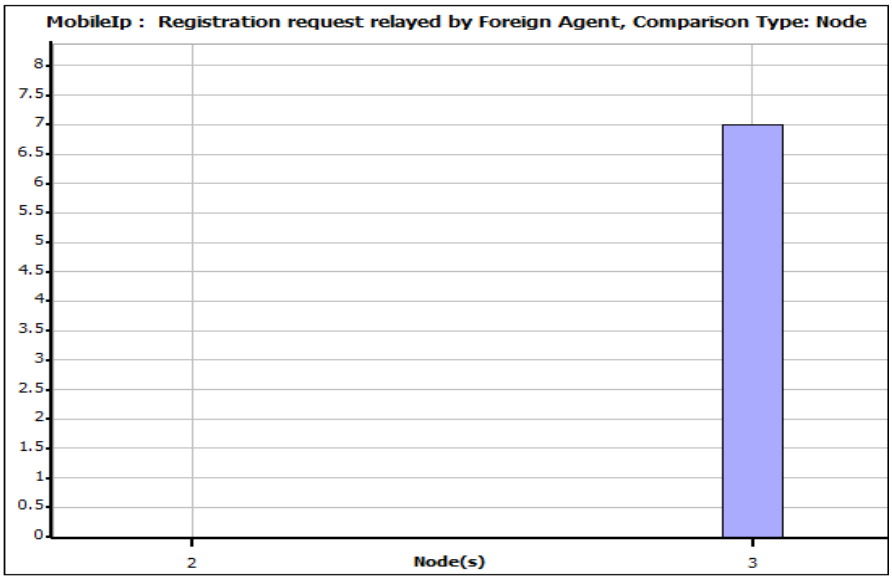


Figura 37. Solicitudes de registro retransmitidas por el FA

### 7.3.4 Solicitudes de registro respondidas Por los HA

Nótese que se respondieron 34 de las 35 solicitudes generadas entre los HA, recordar que el nodo 3 (FA) actúa como HA en la red 2.

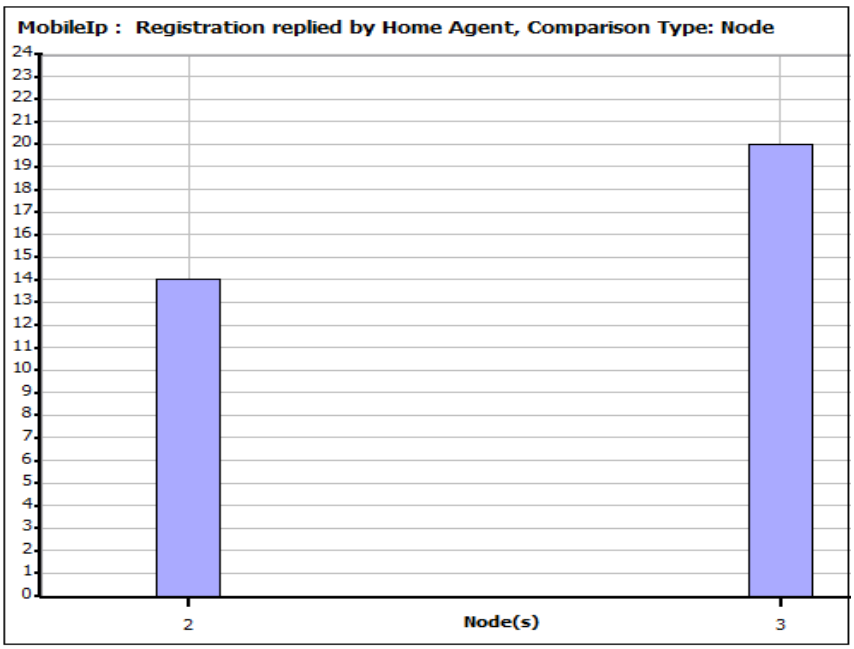


Figura 38. Solicitudes de registro respondidas Por los HA

### 7.3.5 Respuestas a Solicitudes de registro aceptadas

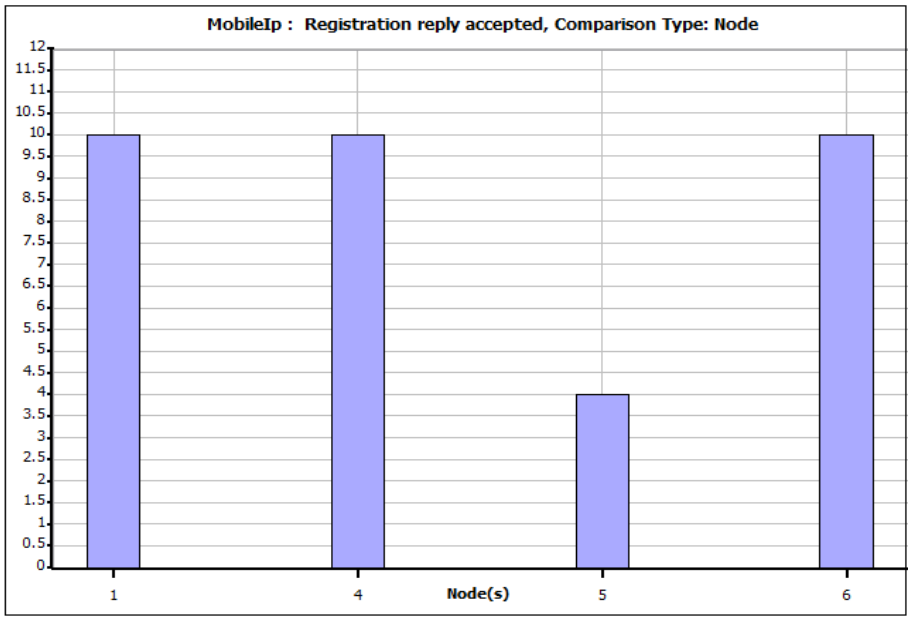


Figura 39. Respuestas a Solicitudes de registro aceptadas

Cada solicitud generada fue respondida, a su vez, cada respuesta de registro fue aceptada por los nodos móviles. Nótese que se respondieron 34 de las 35 solicitudes generadas.

### 7.3.6 Respuestas a solicitud de registro retransmitidas por el FA

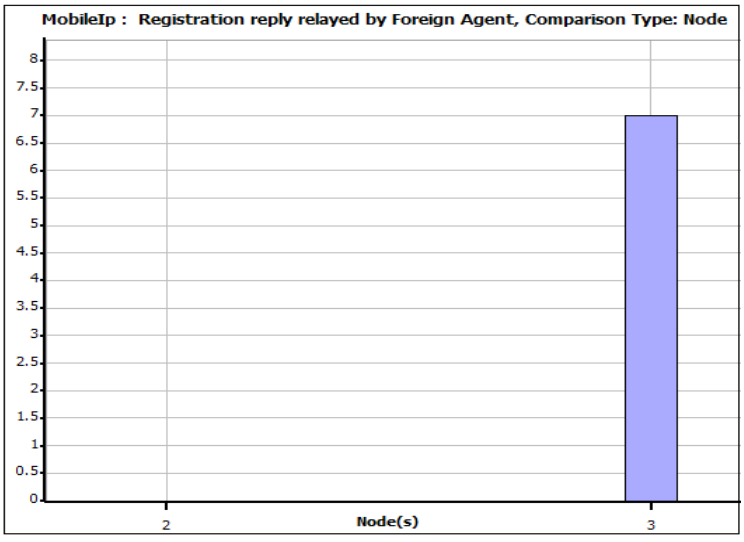


Figura 40. Respuestas a solicitud de registro retransmitidas por el FA.

Luego de recibir la respuesta de parte del HA a las solicitudes de los MN's, el Foreign Agent comunica dichas respuestas a sus nodos móviles visitantes para así completar la fase de registro y permitir que el nodo móvil haga parte ahora de la red foránea. Note que el FA retransmitió la respuesta en 7 ocasiones.

# 8. CONCLUSIONES

- El estudio basado en Mobile IP permitió conocer las capacidades de este protocolo como solución a los desafíos de movilidad a los que se encuentran tanto usuarios, como también, las mismas redes Wireless en expansión. Una transferencia de datos con bajas perdidas indica una alta confiabilidad, mientras que la transparencia del protocolo, permite al usuario permanecer inadvertido.

- El modelo utilizado en la simulación permitió verificar la manera en que el protocolo se integra con la capa de red, además de la manera en que utiliza otros protocolos y mecanismos para funcionar, por ejemplo, la manera en que Mobile IP utiliza ICMP para descubrir los agentes de movilidad.

- Se demostró que los escenarios de Mobile IP incluyen incluso aquellos que son más simples, lo cual deja ver que este protocolo no demanda una gran capacidad por parte de los componentes de red.

- Los conceptos aprendidos durante el curso de formación (MINOR) fueron aplicados en gran parte de este trabajo, permitiendo extender los alcances del curso a este valioso documento.

## REFERENCIAS


CISCO Systems. “Cisco IOS IP configuration Guide”. Release 12.2. Pag 205.

Taeyeon Park y Arek Dadej. “OPNET Simulation Modeling and Analysis of Enhanced Mobile IP”.

Toni Janevski y Ivan Petrov. “Analysis of Mobile IP for NS-2”.

David Cortés Polo y Carlos Vecino de Casas. “Análisis y optimización del Handover en reded MobileIP”.

Scalable Networks. “QualNet 5.0.2Wireless Model Library”

RFC 2002 “IP Mobility Support”
http://www.ietf.org/rfc/rfc2002.txt

RFC 792 “Internet Control Message Protocol”
http://www.faqs.org/rfcs/rfc792.html

RFC 2003 “IP Encapsulation within IP”
http://www.faqs.org/rfcs/rfc2003.html

# ANEXOS

ANEXO A:

```
# ***** QualNet Configuration File *****


#********************General Settings**********************************

VERSION 5.0
EXPERIMENT-NAME QualNet
EXPERIMENT-COMMENT None
SIMULATION-TIME 190S
SEED 1
GUI-BACKGROUND-IMAGE-FILENAME
C:/snt/qualnet/5.0/scenarios/advanced_wireless/WiMAXHomeToOffice/LA.jpg

#********************Parallel Settings**********************************

PARTITION-SCHEME AUTO

#********************ATM Configuration**********************************

DUMMY-ATM-LOGICAL-SUBNET-CONFIGURED NO
ATM-STATIC-ROUTE NO

#********************Dynamic Parameters**********************************

DYNAMIC-ENABLED NO

#*****************************Terrain**********************************

COORDINATE-SYSTEM CARTESIAN
TERRAIN-DIMENSIONS (1000, 1000)
DUMMY-ALTITUDES (1500, 0)
DUMMY-ENABLE-URBAN-TERRAIN-FEATURE NO
WEATHER-MOBILITY-INTERVAL 100MS

#********************Channel Properties**********************************

PROPAGATION-CHANNEL-FREQUENCY[0] 2400000000
```

PROPAGATION-MODEL[0] STATISTICAL
PROPAGATION-PATHLOSS-MODEL[0] TWO-RAY
PROPAGATION-SHADOWING-MODEL[0] CONSTANT
PROPAGATION-SHADOWING-MEAN[0] 4.0
PROPAGATION-FADING-MODEL[0] NONE
PROPAGATION-LIMIT[0] -111.0
PROPAGATION-MAX-DISTANCE[0] 0
PROPAGATION-COMMUNICATION-PROXIMITY[0] 400
PROPAGATION-PROFILE-UPDATE-RATIO[0] 0.0

#**********Mobility and Placement**********

NODE-PLACEMENT FILE
NODE-POSITION-FILE ipmobil.nodes
MOBILITY NONE

#**********STATISTICS**********

PHY-LAYER-STATISTICS YES
MAC-LAYER-STATISTICS YES
ACCESS-LIST-STATISTICS NO
ARP-STATISTICS YES
ROUTING-STATISTICS YES
POLICY-ROUTING-STATISTICS NO
QOSPF-STATISTICS NO
ROUTE-REDISTRIBUTION-STATISTICS NO
EXTERIOR-GATEWAY-PROTOCOL-STATISTICS YES
NETWORK-LAYER-STATISTICS YES
INPUT-QUEUE-STATISTICS NO
INPUT-SCHEDULER-STATISTICS NO
QUEUE-STATISTICS YES
SCHEDULER-STATISTICS NO
SCHEDULER-GRAPH-STATISTICS NO
DIFFSERV-EDGE-ROUTER-STATISTICS NO
ICMP-STATISTICS YES
IGMP-STATISTICS NO
NDP-STATISTICS NO
MOBILE-IP-STATISTICS YES
TCP-STATISTICS YES
UDP-STATISTICS YES
RSVP-STATISTICS NO
SRM-STATISTICS NO
RTP-STATISTICS NO

```
APPLICATION-STATISTICS YES
BATTERY-MODEL-STATISTICS NO
ENERGY-MODEL-STATISTICS YES
MOBILITY-STATISTICS NO
CELLULAR-STATISTICS YES
GSM-STATISTICS NO
VOIP-SIGNALLING-STATISTICS NO
SWITCH-PORT-STATISTICS NO
SWITCH-SCHEDULER-STATISTICS NO
SWITCH-QUEUE-STATISTICS NO
MPLS-STATISTICS NO
MPLS-LDP-STATISTICS NO
HOST-STATISTICS NO

#**********PACKET
TRACING**********

PACKET-TRACE NO
ACCESS-LIST-TRACE NO

#**********Supplemental Files**********

APP-CONFIG-FILE ipmobil.app
DUMMY-USER-PROFILE-FILE-NUMBER 0
DUMMY-TRAFFIC-PATTERN-FILE-NUMBER 0
DUMMY-ARBITRARY-DISTRIBUTION-FILE-NUMBER 0

#**********HLA Interface**********

HLA NO

#**********DIS Interface**********

DIS NO

#**********STK Interface**********

STK-ENABLED NO

#**********Physical Layer**********

PHY-LISTENABLE-CHANNEL-MASK 1
PHY-LISTENING-CHANNEL-MASK 1
```

PHY-MODEL PHY802.11b
PHY802.11-AUTO-RATE-FALLBACK NO
PHY802.11-DATA-RATE 2000000
PHY802.11b-TX-POWER--1MBPS 15.0
PHY802.11b-TX-POWER--2MBPS 15.0
PHY802.11b-TX-POWER--6MBPS 15.0
PHY802.11b-TX-POWER-11MBPS 15.0
PHY802.11b-RX-SENSITIVITY--1MBPS -94.0
PHY802.11b-RX-SENSITIVITY--2MBPS -91.0
PHY802.11b-RX-SENSITIVITY--6MBPS -87.0
PHY802.11b-RX-SENSITIVITY-11MBPS -83.0
PHY802.11-ESTIMATED-DIRECTIONAL-ANTENNA-GAIN 15.0
PHY-RX-MODEL PHY802.11b
ANTENNA-GAIN 0.0
ANTENNA-HEIGHT 1.5
ANTENNA-EFFICIENCY 0.8
ANTENNA-MISMATCH-LOSS 0.3
ANTENNA-CABLE-LOSS 0.0
ANTENNA-CONNECTION-LOSS 0.2
ANTENNA-MODEL OMNIDIRECTIONAL
PHY-TEMPERATURE 290.0
PHY-NOISE-FACTOR 10.0
ENERGY-MODEL-SPECIFICATION NONE

#**********MAC Layer**********

LINK-MAC-PROTOCOL ABSTRACT
LINK-PROPAGATION-DELAY 1MS
LINK-BANDWIDTH 10000000
LINK-HEADER-SIZE-IN-BITS 224
LINK-TX-FREQUENCY 13170000000
LINK-RX-FREQUENCY 13170000000
LINK-TX-ANTENNA-HEIGHT 30
LINK-RX-ANTENNA-HEIGHT 30
LINK-TX-ANTENNA-DISH-DIAMETER 0.8
LINK-RX-ANTENNA-DISH-DIAMETER 0.8
LINK-TX-ANTENNA-CABLE-LOSS 1.5
LINK-RX-ANTENNA-CABLE-LOSS 1.5
LINK-TX-POWER 30
LINK-RX-SENSITIVITY -80
LINK-NOISE-TEMPERATURE 290
LINK-NOISE-FACTOR 4
LINK-TERRAIN-TYPE PLAINS

```
LINK-PROPAGATION-RAIN-INTENSITY 0
LINK-PROPAGATION-TEMPERATURE 25
LINK-PROPAGATION-SAMPLING-DISTANCE 100
LINK-PROPAGATION-CLIMATE 1
LINK-PROPAGATION-REFRACTIVITY 360
LINK-PROPAGATION-PERMITTIVITY 15
LINK-PROPAGATION-CONDUCTIVITY 0.005
LINK-PROPAGATION-HUMIDITY 50
LINK-PERCENTAGE-TIME-REFRACTIVITY-GRADIENT-LESS-STANDARD  15
MAC-PROTOCOL MACDOT11
MAC-DOT11-SHORT-PACKET-TRANSMIT-LIMIT 7
MAC-DOT11-LONG-PACKET-TRANSMIT-LIMIT 4
MAC-DOT11-RTS-THRESHOLD 0
MAC-DOT11-STOP-RECEIVING-AFTER-HEADER-MODE NO
MAC-DOT11-ASSOCIATION NONE
MAC-DOT11-IBSS-SUPPORT-PS-MODE NO
MAC-DOT11-DIRECTIONAL-ANTENNA-MODE NO
MAC-SECURITY-PROTOCOL NO
WORMHOLE-VICTIM-COUNT-TURNAROUND-TIME NO
MAC-PROPAGATION-DELAY 1US

#***************Schedulers and Queues**********************************

IP-QUEUE-PRIORITY-INPUT-QUEUE-SIZE 150000
IP-QUEUE-SCHEDULER STRICT-PRIORITY
IP-QUEUE-NUM-PRIORITIES 3
IP-QUEUE-PRIORITY-QUEUE-SIZE 150000
QUEUE-WEIGHT 0
IP-QUEUE-TYPE FIFO

#*******************QoS Configuration**********************************


#*********************Network Security**********************************

IPSEC-ENABLED NO
ISAKMP-SERVER NO
CERTIFICATE-ENABLED NO
EAVESDROP-ENABLED NO
AUDIT-ENABLED NO

#************************ROUTER
MODEL**********************************
```

```
DUMMY-ROUTER-TYPE USER-SPECIFIED
DUMMY-PARAM NO

#**********NETWORK
LAYER**********

NETWORK-PROTOCOL IP
IP-ENABLE-LOOPBACK YES
IP-LOOPBACK-ADDRESS 127.0.0.1
IP-FRAGMENT-HOLD-TIME 15S
IP-FRAGMENTATION-UNIT 2048
ECN NO
ICMP NO
IPv6-ENABLE-6to4-TUNNELING NO

#**********ROUTING
PROTOCOL**********

ROUTING-PROTOCOL BELLMANFORD
STATIC-ROUTE NO
DEFAULT-ROUTE NO
HSRP-PROTOCOL NO

#**********TRANSPORT**********
**

TRANSPORT-PROTOCOL-RSVP YES
GUI_DUMMY_CONFIG_TCP YES
TCP LITE
TCP-USE-RFC1323 NO
TCP-DELAY-SHORT-PACKETS-ACKS NO
TCP-USE-NAGLE-ALGORITHM YES
TCP-USE-KEEPALIVE-PROBES YES
TCP-USE-OPTIONS YES
TCP-DELAY-ACKS YES
TCP-MSS 512
TCP-SEND-BUFFER 16384
TCP-RECEIVE-BUFFER 16384

#**********MPLS Specs**********

MPLS-PROTOCOL NO
```

```
#*******************Application Layer**********************************

DUMMY-VOIP-APPLICATION-EXISTS NO
RTP-ENABLED NO

#***********************USER
BEHAVIOR***********************************

DUMMY-UBEE-ENABLED NO

#***********************Battery Models*********************************

BATTERY-MODEL NONE

#******************Adaptation Protocol*********************************

ADAPTATION-PROTOCOL AAL5
ATM-CONNECTION-REFRESH-TIME 5M
ATM-CONNECTION-TIMEOUT-TIME 1M

#****************** [Wireless Subnet] *********************************

SUBNET N16-172.25.0.0 {1, 2, 5} 180.158 174.224 0
[ N16-172.25.0.0 ] GUI-NODE-2D-ICON
C:/snt/qualnet/5.0/scenarios/advanced_wireless/WiMAXHomeToOffice/home_office.png

#***********************Physical Layer*********************************

[ N16-172.25.0.0 ] PHY-LISTENABLE-CHANNEL-MASK[0] 1
[ N16-172.25.0.0 ] PHY-LISTENING-CHANNEL-MASK[0] 1
[ N16-172.25.0.0 ] PHY-MODEL PHY802.11b
[ N16-172.25.0.0 ] PHY802.11-AUTO-RATE-FALLBACK NO
[ N16-172.25.0.0 ] PHY802.11-DATA-RATE 2000000
[ N16-172.25.0.0 ] PHY802.11b-TX-POWER--1MBPS 15.0
[ N16-172.25.0.0 ] PHY802.11b-TX-POWER--2MBPS 15.0
[ N16-172.25.0.0 ] PHY802.11b-TX-POWER--6MBPS 15.0
[ N16-172.25.0.0 ] PHY802.11b-TX-POWER-11MBPS 15.0
[ N16-172.25.0.0 ] PHY802.11b-RX-SENSITIVITY--1MBPS -94.0
[ N16-172.25.0.0 ] PHY802.11b-RX-SENSITIVITY--2MBPS -91.0
[ N16-172.25.0.0 ] PHY802.11b-RX-SENSITIVITY--6MBPS -87.0
[ N16-172.25.0.0 ] PHY802.11b-RX-SENSITIVITY-11MBPS -83.0
[ N16-172.25.0.0 ] PHY802.11-ESTIMATED-DIRECTIONAL-ANTENNA-GAIN 15.0
```

[ N16-172.25.0.0 ] PHY-RX-MODEL PHY802.11b
[ N16-172.25.0.0 ] ANTENNA-GAIN 0.0
[ N16-172.25.0.0 ] ANTENNA-HEIGHT 1.5
[ N16-172.25.0.0 ] ANTENNA-EFFICIENCY 0.8
[ N16-172.25.0.0 ] ANTENNA-MISMATCH-LOSS 0.3
[ N16-172.25.0.0 ] ANTENNA-CABLE-LOSS 0.0
[ N16-172.25.0.0 ] ANTENNA-CONNECTION-LOSS 0.2
[ N16-172.25.0.0 ] ANTENNA-MODEL OMNIDIRECTIONAL

#**********MAC Layer**********

[ N16-172.25.0.0 ] MAC-PROTOCOL MACDOT11
[ N16-172.25.0.0 ] MAC-DOT11-SHORT-PACKET-TRANSMIT-LIMIT 7
[ N16-172.25.0.0 ] MAC-DOT11-LONG-PACKET-TRANSMIT-LIMIT 4
[ N16-172.25.0.0 ] MAC-DOT11-RTS-THRESHOLD 0
[ N16-172.25.0.0 ] MAC-DOT11-STOP-RECEIVING-AFTER-HEADER-MODE NO
[ N16-172.25.0.0 ] MAC-DOT11-ASSOCIATION NONE
[ N16-172.25.0.0 ] MAC-DOT11-IBSS-SUPPORT-PS-MODE NO
[ N16-172.25.0.0 ] MAC-DOT11-DIRECTIONAL-ANTENNA-MODE NO
[ N16-172.25.0.0 ] MAC-SECURITY-PROTOCOL NO
[ N16-172.25.0.0 ] WORMHOLE-VICTIM-COUNT-TURNAROUND-TIME NO

#**********NETWORK
LAYER**********

[ N16-172.25.0.0 ] NETWORK-PROTOCOL IP
[ N16-172.25.0.0 ] MOBILE-IP YES
[ N16-172.25.0.0 ] HOME-AGENT {2 }
[ N16-172.25.0.0 ] FOREIGN-AGENT {2}
[ N16-172.25.0.0 ] MOBILE-NODE {1,5 }

#********* [Default Wireless Subnet] **********

#********** [Wireless Subnet] **********

SUBNET N8-192.168.0.0 {3, 4, 6} 699.976 435.319 0
[ N8-192.168.0.0 ] GUI-NODE-2D-ICON
C:/snt/qualnet/5.0/scenarios/advanced_wireless/WiMAXHomeToOffice/telecommuter_house.png

#**********Physical Layer**********

[ N8-192.168.0.0 ] PHY-LISTENABLE-CHANNEL-MASK[0] 1
[ N8-192.168.0.0 ] PHY-LISTENING-CHANNEL-MASK[0] 1
[ N8-192.168.0.0 ] PHY-MODEL PHY802.11b
[ N8-192.168.0.0 ] PHY802.11-AUTO-RATE-FALLBACK NO
[ N8-192.168.0.0 ] PHY802.11-DATA-RATE 2000000
[ N8-192.168.0.0 ] PHY802.11b-TX-POWER--1MBPS 15.0
[ N8-192.168.0.0 ] PHY802.11b-TX-POWER--2MBPS 15.0
[ N8-192.168.0.0 ] PHY802.11b-TX-POWER--6MBPS 15.0
[ N8-192.168.0.0 ] PHY802.11b-TX-POWER-11MBPS 15.0
[ N8-192.168.0.0 ] PHY802.11b-RX-SENSITIVITY--1MBPS -94.0
[ N8-192.168.0.0 ] PHY802.11b-RX-SENSITIVITY--2MBPS -91.0
[ N8-192.168.0.0 ] PHY802.11b-RX-SENSITIVITY--6MBPS -87.0
[ N8-192.168.0.0 ] PHY802.11b-RX-SENSITIVITY-11MBPS -83.0
[ N8-192.168.0.0 ] PHY802.11-ESTIMATED-DIRECTIONAL-ANTENNA-GAIN 15.0
[ N8-192.168.0.0 ] PHY-RX-MODEL PHY802.11b
[ N8-192.168.0.0 ] ANTENNA-GAIN 0.0
[ N8-192.168.0.0 ] ANTENNA-HEIGHT 1.5
[ N8-192.168.0.0 ] ANTENNA-EFFICIENCY 0.8
[ N8-192.168.0.0 ] ANTENNA-MISMATCH-LOSS 0.3
[ N8-192.168.0.0 ] ANTENNA-CABLE-LOSS 0.0
[ N8-192.168.0.0 ] ANTENNA-CONNECTION-LOSS 0.2
[ N8-192.168.0.0 ] ANTENNA-MODEL OMNIDIRECTIONAL

#**********MAC Layer**********

[ N8-192.168.0.0 ] MAC-PROTOCOL MACDOT11
[ N8-192.168.0.0 ] MAC-DOT11-SHORT-PACKET-TRANSMIT-LIMIT 7
[ N8-192.168.0.0 ] MAC-DOT11-LONG-PACKET-TRANSMIT-LIMIT 4
[ N8-192.168.0.0 ] MAC-DOT11-RTS-THRESHOLD 0
[ N8-192.168.0.0 ] MAC-DOT11-STOP-RECEIVING-AFTER-HEADER-MODE NO
[ N8-192.168.0.0 ] MAC-DOT11-ASSOCIATION NONE
[ N8-192.168.0.0 ] MAC-DOT11-IBSS-SUPPORT-PS-MODE NO
[ N8-192.168.0.0 ] MAC-DOT11-DIRECTIONAL-ANTENNA-MODE NO
[ N8-192.168.0.0 ] MAC-SECURITY-PROTOCOL NO
[ N8-192.168.0.0 ] WORMHOLE-VICTIM-COUNT-TURNAROUND-TIME NO

#**********NETWORK
LAYER**********

[ N8-192.168.0.0 ] NETWORK-PROTOCOL IP
[ N8-192.168.0.0 ] MOBILE-IP YES

```
[ N8-192.168.0.0 ] HOME-AGENT {3 }
[ N8-192.168.0.0 ] FOREIGN-AGENT {3}
[ N8-192.168.0.0 ] MOBILE-NODE {4,6}


#**************************** [Link] **********************************

LINK N8-190.0.2.0 { 2, 3 }

#******POINT TO POINT LINK
PROPERTIES**********************************

[ 190.0.2.1 190.0.2.2 ] LINK-PHY-TYPE WIRED
[ 190.0.2.1 190.0.2.2 ] LINK-MAC-PROTOCOL ABSTRACT
[ 190.0.2.1 190.0.2.2 ] DUMMY-GUI-SYMMETRIC-LINK YES
[ 190.0.2.1 190.0.2.2 ] LINK-PROPAGATION-DELAY 1MS
[ 190.0.2.1 190.0.2.2 ] LINK-BANDWIDTH 10000000
[ 190.0.2.1 190.0.2.2 ] LINK-HEADER-SIZE-IN-BITS 224
[ 190.0.2.1 190.0.2.2 ] SWITCH-STATION-VLAN-ID 1
[ 190.0.2.1 190.0.2.2 ] SWITCH-STATION-VLAN-TAGGING NO

#*********************Network Protocol***********************************

[ 190.0.2.1 190.0.2.2 ] NETWORK-PROTOCOL IP

#*********************ROUTING
PROTOCOL***********************************

[ 190.0.2.1 190.0.2.2 ] ROUTING-PROTOCOL BELLMANFORD
[ 190.0.2.1 190.0.2.2 ] DUMMY-GATEWAY-CONFIGURATION NO

#*********************BGP Configuration***********************************

[ 190.0.2.1 190.0.2.2 ] SYNCHRONIZATION YES

#*************Interface Configuration***********************************


[1] NETWORK-PROTOCOL[0]       IP

[1] IP-SUBNET-MASK[0]         255.255.0.0
[1] IP-ADDRESS[0]             172.25.0.1
```

[2] NETWORK-PROTOCOL[0] IP

[2] IP-SUBNET-MASK[0] 255.255.0.0
[2] IP-ADDRESS[0] 172.25.0.2

[2] NETWORK-PROTOCOL[1] IP
[2] IP-ADDRESS[1] 190.0.2.1

[3] NETWORK-PROTOCOL[0] IP

[3] IP-SUBNET-MASK[0] 255.255.255.0
[3] IP-ADDRESS[0] 192.168.0.1

[3] NETWORK-PROTOCOL[1] IP
[3] IP-ADDRESS[1] 190.0.2.2

[4] NETWORK-PROTOCOL[0] IP

[4] IP-SUBNET-MASK[0] 255.255.255.0
[4] IP-ADDRESS[0] 192.168.0.2

[5] NETWORK-PROTOCOL[0] IP

[5] IP-SUBNET-MASK[0] 255.255.0.0
[5] IP-ADDRESS[0] 172.25.0.3

[6] NETWORK-PROTOCOL[0] IP

[6] IP-SUBNET-MASK[0] 255.255.255.0
[6] IP-ADDRESS[0] 192.168.0.3
[172.25.0.1 172.25.0.2 190.0.2.1 192.168.0.1 190.0.2.2 192.168.0.2 172.25.0.3 192.168.0.3] IP-QUEUE-PRIORITY-QUEUE-SIZE[0] 150000
[172.25.0.1 172.25.0.2 190.0.2.1 192.168.0.1 190.0.2.2 192.168.0.2 172.25.0.3 192.168.0.3] IP-QUEUE-TYPE[0] FIFO
[172.25.0.1 172.25.0.2 190.0.2.1 192.168.0.1 190.0.2.2 192.168.0.2 172.25.0.3 192.168.0.3] IP-QUEUE-PRIORITY-QUEUE-SIZE[2] 150000
[172.25.0.1 172.25.0.2 190.0.2.1 192.168.0.1 190.0.2.2 192.168.0.2 172.25.0.3 192.168.0.3] IP-QUEUE-TYPE[1] FIFO
[172.25.0.1 172.25.0.2 190.0.2.1 192.168.0.1 190.0.2.2 192.168.0.2 172.25.0.3 192.168.0.3] IP-QUEUE-PRIORITY-QUEUE-SIZE[1] 150000
[172.25.0.1 172.25.0.2 190.0.2.1 192.168.0.1 190.0.2.2 192.168.0.2 172.25.0.3 192.168.0.3] IP-QUEUE-TYPE[2] FIFO

#**********Hierarchy Configuration**********

#**********Node Configuration**********

[2 3] STATIC-ROUTE-FILE C:/snt/qualnet/5.0/scenarios/user/ipmobil/ipmobil.routes-static
[1] GUI-NODE-2D-ICON C:/Users/ING_RAUL/Desktop/car.png
[2 3] GUI-NODE-2D-ICON C:/snt/qualnet/5.0/gui/icons/devices/router-color.png
[4] GUI-NODE-2D-ICON C:/Users/ING_RAUL/Desktop/2659277.jpg
[5] GUI-NODE-2D-ICON C:/snt/qualnet/5.0/gui/icons/devices/SWIII-1550-Portable.png
[6] GUI-NODE-2D-ICON C:/Users/ING_RAUL/Desktop/2659277.jpg
[1 thru 6] NODE-PLACEMENT FILE
[1 thru 4] ICMP-MAX-NUM-SOLICITATION 3
[5] ICMP-MAX-NUM-SOLICITATION 5
[6] ICMP-MAX-NUM-SOLICITATION 3
[1] MOBILITY FILE
[4 thru 6] MOBILITY FILE
[1 thru 6] NETWORK-PROTOCOL IP
[1] MOBILITY-POSITION-GRANULARITY 1.0
[4 thru 6] MOBILITY-POSITION-GRANULARITY 1.0
[1 thru 6] IP-FRAGMENT-HOLD-TIME 15S
[1 thru 6] ICMP YES
[1 thru 6] IP-LOOPBACK-ADDRESS 127.0.0.1
[1] ROUTING-PROTOCOL NONE
[2 3] ROUTING-PROTOCOL OSPFv2
[4 thru 6] ROUTING-PROTOCOL NONE
[1] HOSTNAME host1
[2] HOSTNAME host2
[3] HOSTNAME host3
[4] HOSTNAME host4
[5] HOSTNAME host5
[6] HOSTNAME host6
[1] ICMP-ROUTER-ADVERTISEMENT-LIFE-TIME 15S
[2] ICMP-ROUTER-ADVERTISEMENT-LIFE-TIME 200S
[3] ICMP-ROUTER-ADVERTISEMENT-LIFE-TIME 40S
[4 thru 6] ICMP-ROUTER-ADVERTISEMENT-LIFE-TIME 15S
[2 3] OSPFv2-INJECT-EXTERNAL-ROUTE NO
[2 3] OSPFv2-STAGGER-START NO

[2 3] OSPFv2-DEFINE-AREA NO
[1 thru 6] ICMP-ROUTER-LIST {2,3}
[1] ICMP-ROUTER-ADVERTISEMENT-MIN-INTERVAL 5S
[2] ICMP-ROUTER-ADVERTISEMENT-MIN-INTERVAL 150S
[3] ICMP-ROUTER-ADVERTISEMENT-MIN-INTERVAL 20S
[4 thru 6] ICMP-ROUTER-ADVERTISEMENT-MIN-INTERVAL 5S
[1] ICMP-ROUTER-ADVERTISEMENT-MAX-INTERVAL 10S
[2] ICMP-ROUTER-ADVERTISEMENT-MAX-INTERVAL 180S
[3] ICMP-ROUTER-ADVERTISEMENT-MAX-INTERVAL 30S
[4 thru 6] ICMP-ROUTER-ADVERTISEMENT-MAX-INTERVAL 10S
[2 3] AS-BOUNDARY-ROUTER NO
[1 thru 6] IP-ENABLE-LOOPBACK YES
[2 3] STATIC-ROUTE YES
[2 3] DEFAULT-ROUTE NO
[1 thru 6] ICMP-ROUTER-DISCOVERY YES
[2 3] QUALITY-OF-SERVICE NONE

#*********Miscellaneous Configuration**********

GUI-DISPLAY-SETTINGS-FILE ipmobil.display