Congreso Argentino en Ciencias de la Computacion - CACiC 2006

Movilidad en IPv4

Javier Díaz
jdiaz@unlp.edu.ar

Mauricio Demasi
mdemasi@cespi.unlp.edu.ar

Matías Robles
mrobles@info.unlp.edu.ar

Germán Vodopivec
vodopivec@cespi.unlp.edu.ar

Laboratorio de Investigaciones en Nueva Tecnologías Informáticas (LINTI)
Facultad de Informática
Universidad Nacional de La Plata

Resumen

El siguiente trabajo tiene como propósito explicar como funciona la movilidad, a nivel de capa de red, usando el protocolo IPv4. El objetivo de la movilidad es proveer conectividad a dispositivos móviles, incluso cuando abandonan su red origen y se mueven a otra con distinta dirección de red. Además, permite que un nodo pueda ser ubicado siempre por su dirección original sin importar su ubicación actual. El análisis del protocolo de movilidad se basó en armar distintas topologías físicas de red, analizar el tráfico intercambiado por los distintos integrantes mientras uno de ellos se mueve hacia otra red con diferente dirección y estudiar como se producía el intercambio de información entre ellos.

Palabras Claves: IPv4, movilidad, Windows, Birdstep Mobile IP

1 INTRODUCCION

Las comunicaciones móviles están comenzando a redefinir la forma en que los usuarios acceden a internet para obtener la información que necesitan. El incremento de la cantidad de dispositivos móviles, como PDAs y notebooks, y el desarrollo de nuevos servicios sobre IP[1], están impulsando la necesidad de estar siempre conectado a nivel IP, aún cuando el usuario se mueva de una red a otra.

Esta movilidad contrasta con la forma en que se usan las direcciones IP, en donde, una dirección se usa para identificar un nodo determinado, además de ser utilizada por los routers para encontrar la ruta hacia el destino. Como la dirección es fija, todo el tráfico destinado a una dirección IP determinada será enviado a un mismo sitio, lo que impide la movilidad. La solución a este problema es Mobile IP [2][3].

Mobile IP es un protocolo de capa de red que permite que un dispositivo móvil mantenga su misma dirección IP, y sus conexiones activas, mientras se mueve de una red a otra.

2 MOBILE IP

Se entiende por movilidad a la capacidad que tiene un nodo para mantener la misma dirección IP, a pesar de que se desplace físicamente a otra red. Esto significa que no importa a que red esté conectado, el nodo sigue siendo accesible a través de una misma dirección IP. Sin esta capacidad, los paquetes destinados a un nodo móvil no podrán llegar a destino mientras dicho nodo se encuentre alejado de su enlace principal.

Para que un nodo tenga la capacidad de movilidad, la misma debe ser habilitada en dicho nodo. En IPv4, las características de movilidad no están incluidas en el protocolo original. Se lo debe actualizar. Esta actualización se debe realizar en todos los participantes del proceso. Existen dos participantes obligatorios, el home agent y el mobile node y, otro que es utilizado según la arquitectura seleccionada, el foreign agent.

Un mobile node es un dispositivo IP, como una notebook, un teléfono celular o una PDA, con capacidad de movilidad habilitado. Mientras se encuentra en su red, conocida como home network, no necesita hacer uso de esa capacidad. Todas las comunicaciones que realiza las hace usando los mecanismos tradicionales de IP, como cualquier otro nodo.

Cuando el mobile node se desplaza hacia otra red, la foreign network, debe registrar su movimiento con un nodo en su red original, el home agent haciendo uso de las propiedades que le brinda la movilidad. Existen dos formas diferentes de realizar el proceso de registración. Una es indirecta, mediante el foreign agent, y la otra es directa entre el mobile node y su home agent.

Pero antes, debe conseguir una dirección IP temporaria correspondiente a la nueva red. Esta dirección se conoce Care-of Address (CoA) y la puede obtener de dos diferentes maneras:

- Foreign Agent Care-of Address: en la red visitada existe un foreign agent(FA) que le provee al mobile node una dirección IP, que es igual a la que tiene asignada la interface del FA en el enlace. Todos los nodos móviles que arriben a la red deberán compartir la misma dirección. No recibe cada uno una dirección particular. La ventaja de este método es que se elimina el problema de la falta de direcciones.

- Co-located Care-of Address: en este método, el mobile node obtiene una dirección IP particular correspondiente a la red visitada a través de algún otro medio, como puede ser DHCP[4]. Como desventaja, este método tiene una cantidad limitada de direcciones disponibles (las que están definidas en el servidor DHCP) pero no se necesita implementar un foreign agent.

La registración es el proceso por el cual el mobile node le informa de su nueva CoA a su home agent, para que éste sepa a donde enviarle las retransmisiones, y solo necesita el intercambio de dos mensajes para realizarse. Estos se envían utilizando el protocolo UDP[5] al puerto 434. Al recibir la solicitud de registración del mobile node, el home agent le contesta indicándole si acepta, o no, el pedido. Si lo rechaza, el proceso se aborta y la movilidad no se concreta. En caso contrario, el home agent comienza a funcionar como *proxy* del mobile node. A partir de este momento, todo el tráfico enviado a la home address del mobile node será interceptado por el home agent, quien lo reenviará a la CoA del mobile node, utilizando un túnel. El otro extremo del túnel lo determina la CoA y puede estar en el foreign agent o en el mismo mobile node. El mensaje original se extrae del túnel y se entrega al destinatario. El algoritmo de encapsulación utilizado para armar los túneles es IP en IP [6] (se pueden utilizar otros algoritmos pero éste debe ser soportado obligatoriamente por todas las implementaciones). En este método, el paquete es encapsulado dentro de otra cabecera IP, que es la cabecera del túnel. Las direcciones IP de esta cabecera indican los extremos del túnel.

En el proceso inverso, el mobile node le puede enviar los mensajes al otro extremo de la conexión, el correspondent node, en forma directa usando los mecanismos de ruteo estándar de Internet, sin utilizar túneles. Los paquetes tienen como source IP la home address del mobile node Se lo llama Ruteo Triangular por el triángulo que forma la conexión entre el mobile node, el home agent y el correspondent node.

Si la foreign network tiene características de seguridad habilitadas, como es el Ingress Filtering [7], el paquete podría no salir de la red. Para evitar esto, se utiliza un procedimiento llamado Reverse Tunneling [8] que funciona de la siguiente manera. El mobile node, o el foreign agent, según quien sea el extremo del túnel, envían los paquetes hacia el home agent, mediante un túnel, poniendo la CoA como Source IP y la dirección del home agent como Destintation IP. Al recibir el paquete, el home agent lo desencapsula y lo reenvía hacia el correspondent node. Esto introduce retardos en la comunicación pero posibilita la integración de movilidad y seguridad.

3 FUNCIONAMIENTO MOBILE IP

Para probar el funcionamiento de Mobile IP se armó el esquema mostrado en el gráfico. Para el home agent y el foreign agent se utilizaron routers Cisco 2600 con el IOS 12.2 [9][10], que tiene soporte para la movilidad, y para el mobile node se utilizó una notebook con Windows 2000. Este SO no trae incorporada la capacidad de movilidad. Para incorporarla se utilizó la aplicación Birdstep Mobile IP [11] (ésta nos fue cedida gentilmente por Birdstep Technology por el lapso de 30 días). Además, a cada router se conectaron dos Access Points Cisco 1200 [12][13]. Las áreas de cobertura de los APs se solapaban para permitirle al mobile node un desplazamiento suave entre ellos y, consecuentemente, el cambio de la home network hacia la foreign network. En la Fig, 1 se muestra la topología de la red de prueba.

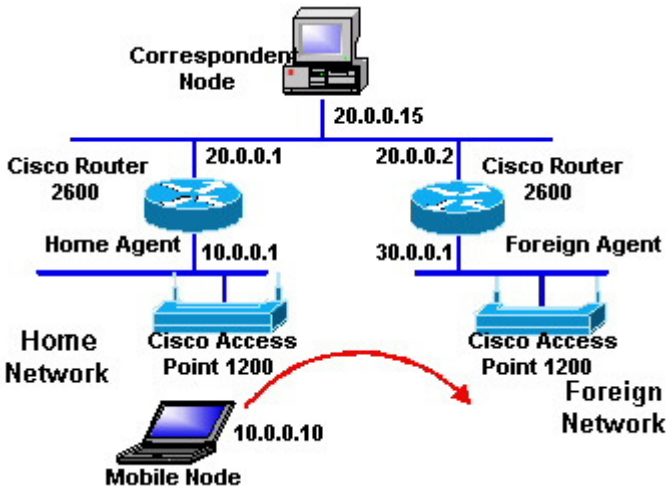

Fig. 1 – Topología red de prueba

Usando esta topología de red, entre otras, se estudió el funcionamiento del protocolo con el router en la foreign network funcionando como foreign agent o como DHCP Server con el fin de probar ambas formas de trabajar. Con los routers configurados adecuadamente, se ejecutaba la aplicación cliente en la notebook, también con la adecuada configuración, y luego nos desplazábamos, con la notebook, desde el área de cobertura de un AP hacia el área de cobertura del otro.

Como se explicó mas arriba, el protocolo IPv4 debe ser actualizado para permitir la movilidad. El home agent es uno de los integrantes del proceso que debe ser actualizado. En primer lugar para que pueda enviar mensajes periódicos a la red, donde anuncia sus servicios, que se conocen como Agent Advertisement[2][3]. Estos son mensajes ICMP Router Advertisement[14] a los que se les añade una extensión, Mobility Agent Advertisement Extensión [2]. Los mensajes se envían a la dirección multicast 224.0.0.11. Además de ser enviados periódicamente, el mobile node puede solicitar tales anuncios mediante un Agent Solicitation, que también es un mensaje ICMP[15] pero, en este caso, es un ICMP Router Solicitation [14]. El mobile node los utiliza para determinar si se encuentra en su home network, o no, proceso que se conoce como Agent Discovery [2][3].

Mientras el mobile node se encuentra en su home network, su funcionamiento es igual al de los demás nodos. La única diferencia que se encontró, es que, al momento de habilitarse la movilidad en el mobile node se registra con su home agent, aunque se encuentre en su home network, luego de ejecutar el Agent Discovery. La herramienta permite definir la dirección IP del home agent para hacer la registración directamente. Si no se definiese, el mobile node ejecuta un proceso conocido como Dynamic Home Agent Assignament[2][3] para encontrar el home agent. Finalizada la registración, el mobile node está en condiciones de desplazarse a otra red, no perder ninguna de las conexiones establecidas y ser encontrado por su dirección IP original

Al desplazarnos con la notebook desde el área de influencia del AP, conectado en la home network, hacia el área correspondiente al AP conectado en la foreign network, el mobile node detecta el cambio de red y, automáticamente después de conectarse al AP de la foreign network, comienza la registración con su home agent que, dependiendo de la infraestructura de la red visitada, es como será realizado.

Si existe un foreign agent, la registración se hace a través de él. El mobile node, mediante el procedimiento Agent Discovery, obtiene la dirección IP del foreign agent y, es a él, a quien le envía los mensajes de registración. A continuación se muestra un mensaje Registration Request el mobile node al foreign agent (algunos campos se han eliminado y en negrita se muestran los campos más importantes):

Internet Protocol
Source: 10.0.0.10
Destination: 30.0.0.1
User Datagram Protocol
Source port: 1651
Destination port: 434
Mobile IP
Message Type: Registration Request
Flags: 0x00
0... .... = Simultaneous Bindings: False
.0.. .... = Broadcast Datagrams: False
..0. .... = Co-located Care-of Address: False
...0 .... = Minimal Encapsulation: False
.... 0... = GRE: False
.... .0.. = Van Jacobson: False
.... ..0. = Reverse Tunneling: False
Lifetime: 36000
Home Address: 10.0.0.10
Home Agent: 10.0.0.1
Care of Address: 30.0.0.1
Identification: Mar 2, 1993 17:39:39,5791 UTC
Extensions
Extension: Mobile-Home Authentication Extension
Extension Type: Mobile-Home Authentication Extension
Extension Length: 20
SPI: 0x00001388
Authenticator: 1F90381ABBB1DA681DA68C355D7A7503

Como se puede ver en el contenido de este paquete, el home agent le envía la solicitud de registración al foreign agent (Destination: 30.0.0.1) pero usando su home address como dirección origen (Source: 10.0.0.10). No obtiene una dirección correspondiente a la foreign network. Además, el mobile node le indica a su home agent que no utilizará Reverse Tunneling, que está usando un foreign agent (..0. .... = Co-located Care-of Address) y que la asociación es por 36000 segundos. También le indica la Care-of Address que deberá utilizar para armar el túnel. Y, para evitar que un falso mobile node se una al home agent, le envía datos de autentificación que deben coincidir con los que el home agent tiene definidos.

El foreign agent recibe el mensaje y lo reenvía al home agent. La dirección de éste la obtiene del campo Home Agent de la cabecera Mobile IP. A continuación se muestra el mensaje:

Internet Protocol
Source: 30.0.0.1
Destination: 10.0.0.1
User Datagram Protocol
Source port: 434
Destination port: 434
Mobile IP
Message Type: Registration Request

Flags: 0x00
0... .... = Simultaneous Bindings: False
.0.. .... = Broadcast Datagrams: False
..0. .... = Co-located Care-of Address: False
...0 .... = Minimal Encapsulation: False
.... 0... = GRE: False
.... .0.. = Van Jacobson: False
.... ..0. = Reverse Tunneling: False
Lifetime: 36000
Home Address: 10.0.0.10
Home Agent: 10.0.0.1
Care of Address: 30.0.0.1
Identification: Mar 2, 1993 17:39:39,5791 UTC
Extensions
Extension: Mobile-Home Authentication Extension
Extension Type: Mobile-Home Authentication Extension
Extension Length: 20
SPI: 0x00001388
Authenticator: 1F90381ABBB1DA681DA68C355D7A7503

Al reenviar el mensaje, el foreign agent pone su dirección IP, la que le dio al mobile node como Care-of Address, como dirección origen del mensajes (Source: 30.0.0.1). Después de procesar el pedido de registración, el home agent le contesta al mobile node a través del foreign agent. El siguiente mensaje es la contestación:

Internet Protocol
Source: 10.0.0.1
Destination: 30.0.0.1
User Datagram Protocol
Source port: 434
Destination port: 434
Mobile IP
Message Type: Registration Reply
Reply Code: Reg Accepted
Lifetime: 36000
Home Address: 10.0.0.10
Home Agent: 10.0.0.1
Identification: Mar 2, 1993 17:39:39,5791 UTC
Extensions
Extension: Mobile-Home Authentication Extension
Extension Type: Mobile-Home Authentication Extension
Extension Length: 20
SPI: 0x00001388
Authenticator: F3B60961E7A7E557F250ED219BCFE835

La respuesta enviada por el home agent indica que la registración fue aceptada. Cuando el foreign agent recibe dicha respuesta, la reenvía al mobile node. A continuación se muestra el mensaje retransmitido:

Internet Protocol
Source: 30.0.0.1
Destination: 10.0.0.10
User Datagram Protocol
Source port: 434

Destination port: 1651
Mobile IP
Message Type: Registration Reply
Reply Code: Reg Accepted
Lifetime: 36000
Home Address: 10.0.0.10
Home Agent: 10.0.0.1
Identification: Mar 2, 1993 17:39:39,5791 UTC
Extensions
Extension: Mobile-Home Authentication Extension
Extension Type: Mobile-Home Authentication Extension
Extension Length: 20
SPI: 0x00001388
Authenticator: F3B60961E7A7E557F250ED219BCFE835

Este es el último mensaje del proceso. A partir del momento que el mobile node lo recibe y procesa, el handover finaliza y el mobile node puede ser ubicado nuevamente por su home address. Todas las conexiones TCP[16] que estaban activas al momento de iniciarse el handover se restablecen, salvo las que se cancelen por timeout.

Por otra parte, si no existe un foreign agent en la red visitada, el mobile node, después de obtener una dirección IP correspondiente a la foreign network, se registra directamente con su home agent. A continuación se muestra el intercambio de mensajes entre ellos:

Internet Protocol
Source: 30.0.0.2
Destination: 10.0.0.1
User Datagram Protocol
Source port: 1743
Destination port: 434
Mobile IP
Message Type: Registration Request
Flags: 0x20
0... .... = Simultaneous Bindings: False
.0.. .... = Broadcast Datagrams: False
..1. .... = Co-located Care-of Address: True
...0 .... = Minimal Encapsulation: False
.... 0... = GRE: False
.... .0.. = Van Jacobson: False
.... ..0. = Reverse Tunneling: False
Lifetime: 65535
Home Address: 10.0.0.10
Home Agent: 10.0.0.1
Care of Address: 30.0.0.2
Identification: Mar 4, 1993 19:11:35,4424 UTC
Extensions
Extension: Mobile-Home Authentication Extension
Extension Type: Mobile-Home Authentication Extension
Extension Length: 20
SPI: 0x00001388
Authenticator: 78B5414D90197AC3E6A8F5CE2D59043A

La dirección IP origen (Source: 30.0.0.2) es una dirección obtenida por DHCP y la dirección destino (Destination: 10.0.0.1) es la dirección del home agent. A diferencia del proceso anterior, se

indica que la Care-of Address es co-located, obtenida por DHCP por ejemplo. La contestación del home agent es directamente al mobile node:

Internet Protocol
Source: 10.0.0.1
Destination: 30.0.0.2
User Datagram Protocol
Source port: 434
Destination port: 1743
Mobile IP
Message Type: Registration Reply
Reply Code: Reg Accepted
Lifetime: 36000
Home Address: 10.0.0.10
Home Agent: 10.0.0.1
Identification: Mar 4, 1993 19:11:35,4424 UTC
Extensions
Extension: Mobile-Home Authentication Extension
Extension Type: Mobile-Home Authentication Extension
Extension Length: 20
SPI: 0x00001388
Authenticator: 81B852287073D732EE2CB7E86CEA4279

Luego de la registración, el home agent debe empezar a funcionar como proxy del mobile node. Por esta razón, envía un mensaje broadcast ARP Gratuitous para que todos los nodos vecinos actualicen su tabla ARP[17]. La actualización consiste en asociar la home address del mobile node con la dirección MAC del home agent. A partir de este momento, todo los mensajes enviados al mobile node serán recibidos por el home agent, quien a su vez, lo retransmitirá, túnel mediante, a la ubicación actual del mobile node. También, el home agent asumirá a responsabilidad de contestar los ARP Request enviados por los demás nodos preguntando por la dirección MAC del mobile node.

Al igual que en el método anterior, a partir de este momento, el mobile node puede volver a comunicarse con un correspondent node, pero el tipo de conexión depende de la infraestructura de la red. Como en el caso de la registración, si existe un foreign agent, el túnel desde el home agent debe terminar en él. A continuación se muestra la captura de un mensaje Ping Request enviado desde el host con la IP 20.0.0.15 hacia el mobile node.

Internet Protocol
Source: 10.0.0.1
Destination: 30.0.0.1
Internet Protocol
Source: 20.0.0.15
Destination: 10.0.0.10
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x435c [correct]
Identifier: 0x0200
Sequence number: 0x0800
Data (32 bytes)

El mensaje original es enviado desde el correspondent node, con IP origen igual a 20.0.0.15,

hacia el mobile node, que tiene la dirección IP 10.0.0.10. Pero, éste ya no se encuentra en su home network, se ha desplazado hacia otra red. El home agent recibe el mensaje en nombre del mobile node y lo reenvía. Para esto, primero lo encapsula en otra cabecera IP, en la cual la dirección IP origen es la del home agent (10.0.0.1) y la de destino es la Care-of Address (30.0.0.1). En este caso, la CoA es la del foreign agent y es el extremo final del túnel. El foreign agent desencapsula el paquete y se lo reenvía al mobile node.

Cuando el mobile node se registró con su home agent le indicó que no va a utilizar Reverse Tunneling. Por esto, la contestación va directamente desde el mobile node al correspondent node, sin pasar por el home agent. A continuación se muestra el mensaje:

Internet Protocol
Source: 10.0.0.10
Destination: 20.0.0.15
Internet Control Message Protocol
Type: 0 (Echo (ping) reply)
Code: 0
Checksum: 0x4b5c [correct]
Identifier: 0x0200
Sequence number: 0x0800
Data (32 bytes)

Si la registración se hace directamente desde el mobile node al home agent, la dirección IP destino de la cabecera externa sería, por ejemplo, la que el mobile node obtuvo por DHCP. Al no existir un foreign agent, el mensaje se reenvía directamente al mobile node, quien al recibirlo, lo desencapsula y lo procesa. A continuación se muestra un mensaje de este tipo.

Internet Protocol
Source: 10.0.0.1
Destination: 30.0.0.2
Internet Protocol
Source: 20.0.0.15
Destination: 10.0.0.10
Internet Control Message Protocol
Type: 8 (Echo (ping) request)
Code: 0
Checksum: 0x405c [correct]
Identifier: 0x0200
Sequence number: 0x0b00
Data (32 bytes)

La contestación del mobile node también es directa al correspondent node.

3.1 Desregistración

Cuando el mobile node regresa a su home network debe dejar de utilizar el home agent para sus comunicaciones. Para desregistrarse, el mobile node debe enviar un mensaje Registration Request con el campo Lifetime igual a 0. El home agent le contesta con Registration Reply indicándole el éxito de la operación.

Antes de enviar el Registration Request, el mobile node debe indicarle al resto de los nodos de su home network que se encuentra nuevamente en ella. Para esto envía un mensaje broadcast ARP Gratuitous para que los nodos vecinos actualicen su tabla ARP asociando nuevamente la

dirección IP original del mobile node con su propia dirección MAC.

3.2 Handover

El proceso de movilidad tiene un punto crítico y es el momento en el que el mobile node se desplaza de una red hacia otra. Esto se conoce como handover [2][3] (o handoff) y es el tiempo transcurrido desde que el mobile node detecta que se encuentra en otra red hasta que se registra exitosamente con su home agent. Si en este preciso momento, el mobile node está intercambiando mensajes con un correspondent node, estos se perderán y deberán ser retransmitidos cuando el proceso de registración finalice o, lo que sería peor aún, la comunicación podría finalizar por un timeout.

Usando una infraestructura con un foreign agent, se midió el tiempo que llevaría el handover en una red como la mostrada mas arriba. El tiempo menor fue de 116 milisegundos, el mayor de 220 milisegundos y el promedio, de las 8 pruebas realizadas fue de 134 milisegundos. De las 8 pruebas realizadas, 5 de ellas estuvieron entre los 116 y los 120 milisegundos.

El tiempo empleado para realizar todo el proceso es bajo, teniendo en cuenta todos los pasos que se deben realizar (desasociarse de un access point, autentificarse y asociarse al nuevo access point, determinar la dirección de la nueva red y registrase con su home agent) pero estos tiempos podrían incrementarse en redes con mucho tráfico o si el mobile node se encuentra en una red alejada de su home agent. Si el tiempo se incrementa demasiado, las conexiones activas podría perderse.

4 CONCLUSIONES

En este trabajo se estudiaron los puntos más importantes de la movilidad en IPv4. El protocolo es una excelente solución al problema que generan los usuarios móviles que necesitan conexión continua a Internet (o cualquier otro red). El problema mayor del protocolo lo presenta el handover y el posterior paso de registración del mobile node con su home agent. Para esto último, necesita intercambiar solo dos paquetes de un tamaño pequeño en el menor tiempo posible. Este intercambio se podría mejorar dándole una prioridad alta en el procesamiento en los routers atravesados por los mensajes.

Otro problema existente, aunque éste es inherente a IPv4, es la posibilidad de no contar con direcciones IP disponibles en algunas de las redes visitadas. Con la implementación de un foreign agent el protocolo soluciona este problema en forma satisfactoria.

El proceso de movilidad es totalmente transparente para las capas superiores de la pila de protocolos, como TCP y UDP.

La aplicación cliente para entornos Windows tiene un funcionamiento aceptable y muy simple de configurar. Permite especificar características de seguridad entre el mobile node y el home agent y, entre el mobile node y el foreign agent. El producto utilizado, Birdstep Mobile IP Client, ofrece una versión de prueba por un período de tiempo de 30 días.

Por último, continuando con este trabajo se están probando distintos tipos de aplicaciones, como pueden ser Voice over IP, streaming, protocolos de transferencias de archivos, etc., sobre mobile IP.

REFERENCIAS

[1] J.B. Popstel, “Internet Protocol”, RFC 791, Septiembre 1981
[2] C. Perkins, “IP Mobility Support for IPv4”, Agosto 2002
[3] Madjid Nakhjiri, “AAA and Network Security for Mobile Access: Radius, Diameter, EAP, OKI and IP Mobility”, Ed. John Wiley, 2005
[4] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, Marzo 1997
[5] J.B. Popstel, “User Datagram Protocol”, RFC 768, Agosto 1980
[6] Perkins, C., "IP Encapsulation within IP", RFC 2003, Octubre 1996
[7] P. Ferguson, “Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing”, RFC 2827, Mayo 2000
[8] G. Montenegro, " Reverse Tunneling for Mobile IP, revised", RFC 3024, Enero 2001
[9] Cisco System, “Understanding Mobile IP”, Noviembre 2005
[10] Cisco System, “Cisco Mobile IP”, White Paper, Junio 2001
[11] Birdstep Technology, “Mobile IP Overview “, Diciembre 2002
[12] IEEE 802.11 – Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications
[13] Cisco Access Point 1200 - http://www.cisco.com/en/US/products/hw/wireless/ps430/index.html
[14] Deering, S., "ICMP Router Discovery Messages", RFC 1256, Septiembre 1991
[15] J.B. Popstel, “Internet Control Message Protocol”, RFC 792, Septiembre 1981
[16] J.B. Popstel, “Transport Control Protocol”, RFC 793, Septiembre 1981
[17] David C. Plummer, “An Ethernet Address Resolution Protocol”, RFC 826, Noviembre 1982