PROTOCOLO DE INTERNET, IP MÓVIL, LA SOLUCIÓN PARA LA MIGRACIÓN DE REDES PRIVADAS A PÚBLICAS

NICOLÁS LÓPEZ MONTOYA

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
EMPRESA SIEMENS S.A.
BOGOTÁ D.C.
2005

PROTOCOLO DE INTERNET, IP MÓVIL, LA SOLUCIÓN PARA LA MIGRACIÓN DE REDES PRIVADAS A PÚBLICAS

NICOLÁS LÓPEZ MONTOYA

Trabajo de grado de investigación para optar al título
de Ingeniero de Telecomunicaciones

Tutor
Jorge Humberto Muñoz
Ingeniero Electrónico

UNIVERSIDAD SANTO TOMÁS
FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES
EMPRESA SIEMENS S.A.
BOGOTÁ D.C.
2005

Nota de aceptación:

_____
_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bogotá, 11/05/05

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

RESUMEN

El presente documento especifica los antecedentes del protocolo IP como el protocolo tal vez, más importante de los últimos tiempos y su estructura interna, así como las ventajas que permiten el enrutamiento transparente de datagramas IP a nodos móviles en Internet. Cada nodo móvil siempre es identificado por su dirección local, a pesar de su punto actual de acople a Internet. Mientras él está situado lejos de su punto local, un nodo móvil está asociado con una dirección temporal, la cual provee información acerca de su punto actual de conexión a Internet. El protocolo provee para el registro la dirección temporal con un agente local. El agente local envía datagramas destinados para el nodo móvil a través de un túnel hacia la dirección temporal. Después de la llegada al final del túnel, cada datagrama es entonces entregado al nodo móvil.

INTRODUCCIÓN

"Los actuales protocolos de internetworking presentan serias complicaciones a la hora de tratar con nodos que disponen de un cierto grado de movilidad entre redes. La mayoría de las versiones del protocolo IP (Internet Protocol) asumen de manera implícita que el punto al cual el nodo se conecta a la red es fijo. Por otra parte, la dirección IP del nodo identifica al mismo de manera unívoca en la red a la que se encuentra conectado. Por consiguiente, cualquier paquete destinado a ese nodo es encaminado en función de la información contenida en la parte de su dirección IP que identifica la red en que está conectado.

Esto implica que un nodo móvil que se desplaza de una red a otra y que mantiene su dirección IP no será localizable en su nueva situación, ya que los paquetes dirigidos hacia este nodo serán encaminados a su antiguo punto de conexión a la red.

El protocolo IP Móvil constituye una mejora del protocolo IP citado anteriormente. Mobile IP o IP Móvil, permite a un nodo circular libremente a través de Internet siendo éste siempre accesible mediante una única dirección IP."[1]

Por otro lado, la constante evolución tan acelerada de los sistemas de comunicaciones y la constante inquietud de los ingenieros y científicos en el sector, ha llevado a que se plantee un problema de integración de las redes terrestres fijas, satelitales e inalámbricas y la manera como se accede hoy en día a ellas.

Los usuarios o consumidores de las diferentes tecnologías, son cada vez más exigentes a la hora de intercambiar información y solicitan no sólo calidad sino también velocidad de transferencia de datos y mayor transparencia, sea cual sea su aplicación.

El desarrollo de nuevos productos para el mercado masivo da pie al progreso de sistemas que soporten tales productos, los cuales están siendo optimizados cada vez más para proveer servicios integrados de banda ancha.

[1] Aparte de la Introducción del documento Mobile IP: una solución para proporcionar movilidad de los terminales en Internet. [Documento en Línea]. 2004. Disponible en Internet < http://acimut.upf.es/moliver/OlL99.pdf >

Por todo lo anterior la rápida evolución globalizada de la sociedad de información, está siendo fomentada por un incremento de la demanda, para unificar servicios integrados. En el pasado, las soluciones de red y sistemas tendieron a ser desarrollados de una manera cerrada e independiente, proveyendo especializadas arquitecturas con flexibilidad limitada. No obstante, debido a la rápida evolución, hay actualmente un incremento en la integración y convergencia de las funciones de red. El éxito de cualquiera de estos nuevos sistemas, depende de la prestación de servicios de bajos costos y soluciones flexibles, que hagan frente a la creciente demanda.

El reto es pues, proveer un conjunto de opciones en términos de servicio, terminales y accesos de red, lo cual es posible de hacer reuniendo diferentes requerimientos y proporcionando flexibilidad, modularidad y capacidad de crecimiento. Esto es lo que hará en un futuro no muy lejano el protocolo IP MÓVIL.

Con el rápido crecimiento y la disponibilidad de las redes de datos móviles, herramientas de comunicaciones móviles y estándares Internet, los trabajadores móviles han encontrado nuevas formas de hacer negocios en el entorno competitivo actual. La necesidad para los trabajadores móviles de acceder a información crítica requiere el acceso a bases de datos corporativas y a aplicaciones Internet/Intranet. Además, la transferencia de mensajes fiable y adecuada, la integridad de mensajes, y la entrega de información personalizada permite al empleado móvil trabajar a altos niveles de productividad. El éxito en las comunicaciones entre trabajadores móviles y su entorno corporativo requiere una correcta combinación de las tecnologías. Desde el punto de vista de los negocios, estas tecnologías deben ser baratas y fáciles de usar. Para la viabilidad a largo plazo, deben basarse en arquitecturas de sistemas abiertos e interfaces industriales estándar. Las redes privadas virtuales han surgido para facilitar soluciones de interconexión a una creciente mano de obra móvil. Una red privada virtual permite a los negociantes facilitar a sus empleados móviles el acceso a la información y aplicaciones corporativas, conectándolos a la empresa utilizando redes públicas, tales como Internet.

Utilizando las redes públicas como backbone de comunicaciones, una red privada virtual proporciona a la empresa una extensión barata, ofreciendo acceso seguro a un entorno abierto de red.

Así pues, el interés por ofrecer movilidad a la red de datos es el resultado de los avances tecnológicos alcanzados en el área de las comunicaciones digitales, que han facilitado accesar redes inalámbricas privadas o globales. Como resultado de este interés, la Internet, esta estudiando mecanismos y procedimientos que permitan el acceso de usuarios móviles. Los mecanismos

estudiados reúnen soluciones a nivel de las capas de red y de transporte. A nivel de la capa de red se esta especificando un nuevo protocolo IP y a nivel de la capa de transporte se ha buscado eliminar las limitaciones cuando se opera en un ambiente móvil. Las soluciones a nivel de red permiten el acceso global y las de transporte ofrecen movilidad a los usuarios.

El IETF (*Internet Engineering Task Force*) es el órgano de la Internet encargado de mantener la integridad de la red, mejorar su desempeño y determinar cuando están siendo demandados nuevos servicios, es por esto que el IETF debe definir los mecanismos y los cambios dentro de la red que permiten movilidad y el acceso global con la calidad necesaria, manteniendo las características de la red.

Los problemas que deben ser resueltos para ofrecer movilidad y acceso global están relacionados con las características de direccionamiento dentro de la red (dirección IP) y a los procedimientos de configuración de los usuarios Internet, DHCP (*Dynamic Host Configuration Protocol*). Con este procedimiento los usuarios: obtienen la dirección lógica y configuran los parámetros que permiten el intercambio de información con otros usuarios o entidades de la red.

El procedimiento de configuración se hace de forma que las direcciones y los parámetros estén fuertemente relacionados, por ejemplo, la compuerta de conexión Ethernet (físico) esta relacionada con la dirección IP, de esta forma si el usuario no consigue accesar la red desde otra compuerta Ethernet, no podrá ingresar a la red.

Como la administración de la red se hace basada en jerarquías (DNS - (*Domain Name System*)) un número IP solamente será valido dentro de su dominio DNS y no conseguirá accesar de forma transparente a la red usando su número IP, sino está dentro de su dominio. La solución probable es asignar una dirección lógica y un número IP (permanentes) en la red de origen (DNS) y adquirir un número temporal en el DNS visitado.

Un número IP temporal trae dificultades relacionadas con la administración, la transmisión sobre la red y la forma como el mismo se adquiere en los DNS visitados.

Otra dificultad se debe a las características del ambiente móvil donde se hace necesario realizar procedimientos de *handoff,* actualización de la posición, etc. Si estos procedimientos no son realizados eficientemente los usuarios pueden experimentar pausas, retardos o interrupción en la comunicación. Estos acontecimientos son considerados por los actuales protocolos OSI de

transporte, como efectos resultados de la congestión de la red, lo que provoca que los mecanismos para control del congestionamiento se accionen. Cada vez que estos mecanismos son accionados el desempeño de la red es degradado. Se puede concluir entonces que los problemas de la red Internet para permitir acceso móvil, están en las capas de red y transporte.

Desde el punto de vista humano, a través del paso de los años el interés del hombre siempre ha sido buscar soluciones a problemas cotidianos, que luego de un estudio detallado y de una investigación han traído como consecuencia la creación de grandes inventos para la humanidad en la mayoría de las veces. En este momento se puede decir que IP Móvil puede llegar a ser un gran invento y esto solo podrá ser comprobado con el paso del tiempo.

La humanidad siempre ha tratado de conseguir lo mejor para vivir, lo cual incluye cosas tan simples como comer, moverse, hacer tareas diarias y hasta comunicarse. Todas estas labores han tenido grandes cambios con el avance tecnológico y este último ha facilitado la vida en el planeta, desde todos los puntos de vista, sin dejar de largo lo referente a los métodos y facilidades de comunicación con el resto de las personas.

Tal vez, se puede decir que desde el inicio de los tiempos el hombre siempre se ha preocupado por comunicar sus sentimientos, sus vivencias, sus conocimientos, su historia, su forma de ser y de actuar y por consiguiente su forma de desarrollarse y sobresalir dentro de un grupo ya sea familiar, de amigos o laboral; es probable que uno de los nichos sociales más relevantes en el cual el hombre debe ser más productivo, más competente y más eficiente es en el grupo de trabajo, pues es allí donde verdaderamente se puede observar la importancia de él y su utilidad. Por tal motivo es necesario que una persona que trabaja en estos tiempos donde la comunicación es algo fundamental, debe sentirse tranquilo, seguro, útil, indispensable dentro de su entorno de trabajo y en constante contacto con la información, independientemente del lugar donde se encuentre.

De esta manera, las tecnologías de la información y de las comunicaciones tales como IP Móvil, pueden brindar al usuario, en este caso, a cualquier persona conectada a una red local, de cualquier empresa en el mundo y con conexión a Internet, la posibilidad de sentirse cómodo, productivo y parte integral de esta última y del grupo de trabajo al cual pertenece sin necesidad de permanecer estático, facilitando su trabajo y fortaleciendo su relación tanto con la compañía para la cual trabaja, como con el resto de las personas conocidas, facilitando también, como algo muy interesante, un acercamiento y una interacción con personas y culturas desconocidas que en determinado momento pueden llegar a servir de soporte mutuo en cualquier aspecto; la persona nunca se sentirá sola o incomunicada por el simple hecho de haber

salido de su puesto de trabajo, entendido este como el sitio donde normalmente recibe la información del resto de las personas. Desde este punto de vista, cualquier invento o creación que facilite y haga sentir a una persona que es valiosa y que no detenga o entorpezca sus labores diarias en cualquier ámbito, ya sea empresarial, familiar, educativo, político o económico, se puede calificar como algo sumamente motivante, imprescindible, manejable, eficaz e importante y hasta trascendental para el desarrollo de la personalidad del ser humano, ya que lo único que trae consigo son beneficios para una mejor calidad de vida.

Así pues, como objetivo del trabajo de profundización de la pasantía, es investigar sobre el protocolo IP Móvil y darlo a conocer de manera profunda, tanto a los estudiantes como a la empresa Siemens que conoce muy vagamente el tema o simplemente no lo conoce. De esta forma se quiere mostrar como una de las nuevas tecnologías que puede llegar a ser la base de futuros sistemas de red, basados en el protocolo IP, el cual es la base del actual Internet.

Por otra parte se pretende mostrar la importancia que puede tener IP Móvil en el sector de las telecomunicaciones en el futuro, con respecto a la flexibilidad en la forma de acceder a las redes, tal como ya se ha mencionado antes y a su utilidad en “la sociedad de la tecnología”, que será la que finalmente permita o no su implementación, su uso y su aceptación.

Además se desea visualizar esta tecnología por medio de la investigación, desde todos los puntos de vista posibles, entre ellos sus antecedentes, su evolución hasta el día de hoy, su relación con otras tecnologías ligadas con IP y su funcionamiento interno y externo; algo de esto ya ha sido desarrollado como parte de esta introducción, pero la idea es profundizar un poco más en cuanto a los mensajes y campos que se manejan en él, algunas consideraciones de importancia como son su seguridad, las extensiones, protocolos utilizados para el correcto funcionamiento y la arquitectura básica.

Finalmente, se describirá el uso y funcionamiento de IP Móvil a través de algunos ejemplos de mensajes estándar y un modelo de implementación en el mundo real mostrando su aplicación, enfocando de manera sencilla y concisa, su utilidad para la sociedad, en un contexto humano y sobretodo sus ventajas para el mejoramiento de la calidad de vida, a lo largo del documento.

1. ANTECEDENTES

Los protocolos actuales de interconexión ya mencionados en el planteamiento general descrito en la introducción, poseen algunas complicaciones cuando deben tratar con hosts móviles entre redes. La mayor cantidad de las versiones del protocolo IP (Internet Protocol) dan por hecho que el punto al cual un host se conecta a la red es fijo.

Además, la dirección IP sirve para identificar el nodo de forma única dentro de la red a la que se encuentra conectado. Es por eso que los paquetes que van hacia este host son encaminados según su dirección y la red a cual está conectado; dicha dirección está dada en el campo de dirección IP dentro del paquete.

Por tal motivo, no será localizable un host móvil que se mueve de una red a otra manteniendo su dirección IP, en su nueva posición, pues los datagramas o paquetes dirigidos hacia él serán enrutados a su punto de conexión antiguo en la red.

IP Móvil es en pocas palabras una nueva versión mejorada del protocolo IP. En IP Móvil un host puede moverse libremente por medio de Internet sin perder su acceso utilizando una dirección IP única. La Internet Engineering Task Force (IETF) propone una arquitectura Mobile IP o IP Móvil que funciona a grandes rasgos, bajo el siguiente concepto: un agente local, denominado Home Agent (HA) y un agente externo, también denominado Foreign Agent (FA) colaboran para permitir que el nodo móvil o Mobile Host (MH) pueda moverse conservando su dirección IP inicial.

El concepto de IP Móvil anteriormente mencionado es el núcleo del presente trabajo y la parte principal la cual será desarrollada con mayor profundidad en las siguientes secciones del mismo.

1.1 MODELO OSI

El modelo OSI (Open System Interconection), como su nombre lo indica, es un estándar para el diseño de redes, el cual define la forma de las comunicaciones en sistemas abiertos. Ver figura 1. Este modelo de referencia, determina

diferentes niveles de comunicación por los cuales viaja la información entre un origen y un destino. Generalmente, la información toma diferentes nombres según el nivel en el que se encuentre. La unidad más simple de información es el bit, luego trama y en el nivel de red toma el nombre de paquete o datagrama. En los niveles superiores del modelo OSI, a esta información se le denomina Unidad de Datos de Protocolo o PDU (Protocol Data Unit) la cual adquiere el nombre completo según el nivel en el que se encuentre; por ejemplo la Unidad de Datos de Protocolo del nivel de Transporte de denomina Unidad de Datos de Trasporte de Protocolo y así sucesivamente según la capa correspondiente.

Figura 1. Capas del modelo OSI

APLICACIÓN
PRESENTACIÓN
SESIÓN
TRANSPORTE
RED
ENLACE
FÍSICO

Autor.

- NIVEL FÍSICO: en este nivel se colocan las señales (información) en forma de bits. Se encarga de interpretar la información que va poner el medio físico. Aquí se definen interfaces físicas, mecánicas, eléctricas, etc. y se determina la manera como se puede conectar al medio físico.

- NIVEL ENLACE: este nivel se encarga de que la comunicación entre dos (2) nodos sea correcta antes de pasar la información al siguiente nivel y también de que esta información no esté duplicada. En este nivel se crean tramas, se hace corrección de errores y control y gestión de tramas.

- NIVEL RED: se encarga de armar y enviar paquetes al nivel superior y de verificar que los paquetes lleguen en el orden correcto para pasar al siguiente nivel. Además, aquí se establecen las rutas adecuadas para llegar al destino, se efectúa direccionamiento y control de congestión. En este nivel se desarrolla lo que hoy se conoce como Internet, haciendo una analogía del nivel de IP del Modelo TCP/IP.

- NIVEL TRANSPORTE: aquí se transporta toda la información completa, a diferencia de las subredes donde se transportan los paquetes uno a uno. Por otro lado, en este nivel del modelo OSI se realiza control de flujo y se establece un camino lógico para llevar la información.

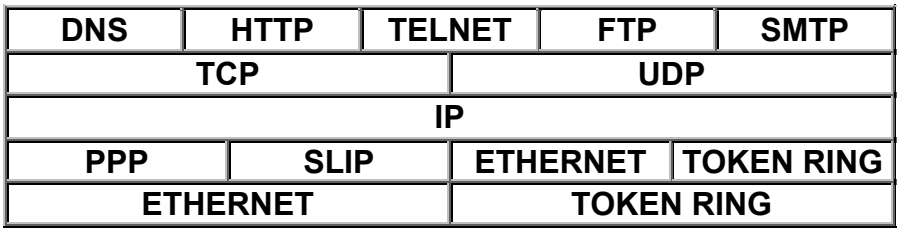
- NIVEL SESIÓN: establece las condiciones de dialogo entre los nodos, es decir que funciona como un moderador de la comunicación. En este nivel también se hace sincronización entre procesos y se determina con quien se establece la comunicación.

- NIVEL PRESENTACIÓN: este nivel hace la transformación de toda la información en forma de bits o binaria (ceros y unos) a un lenguaje que pueda ser leído y entendido por el usuario. En otras palabras, allí se le da formato a los datos, se hace traducción de código y se aplican los conceptos de sintaxis y semántica.

- NIVEL APLICACIÓN: se encarga de presentar el mensaje que fue enviado, con formato de aplicación de usuario. En este nivel se ejecuta el software, el cual permite visualizar la información real. Se considera la puerta de entrada a OSI para el usuario.

1.2 MODELO TCP/IP

Figura 2. Modelo TCP/IP



Autor.

1.3 PROTOCOLO IP

"La capa de red en Internet: en la capa de red, Internet puede verse como un conjunto de subredes, o sistemas autónomos (AS, Autonomous System) interconectados. No hay una estructura real, pero existen varios backbone principales. Estos se construyen a partir de líneas de alto ancho de banda y enrutadores rápidos. Conectadas a los backbone hay redes regionales (de nivel medio), y conectadas a estas redes regionales están las LAN. El "pegamento" que mantiene unida a Internet es el protocolo de capa de red, IP (Internet Protocol o protocolo de Internet).

La comunicación en Internet funciona como sigue. La capa de transporte toma corrientes de datos y las divide en datagramas. En teoría, los datagramas pueden ser de hasta 64 Kbytes cada uno, pero en la práctica por lo general son de unos 1500 bytes. Cada datagrama se transmite a través de Internet, posiblemente fragmentándose en unidades más pequeñas en el camino. Cuando todas las piezas llegan finalmente a la máquina de destino, son reensambladas por la capa de red, dejando el datagrama original. Este datagrama entonces es entregado a la capa de transporte, que lo introduce en la corriente de entrada del proceso receptor.

El protocolo IP: un datagrama IP consiste en una parte de cabecera y una parte de texto. La cabecera tiene una parte fija de 20 bytes y una parte opcional de longitud variable. El formato de la cabecera se muestra en la figura 3."[2]

El protocolo IP es el software que implementa el mecanismo de entrega de paquetes sin conexión y no confiable (técnica del mejor esfuerzo).
El protocolo IP cubre tres aspectos importantes:

- Define la unidad básica para la transferencia de datos en una inter-red, especificando el formato exacto de un Datagrama IP.
- Realiza las funciones de enrutamiento.
- Define las reglas para que los Host y Routers procesen paquetes, los descarten o generen mensajes de error.

El Datagrama IP: el esquema de envío de IP es similar al que se emplea en la capa de Acceso a red. En esta última se envían Tramas formadas por un Encabezado y los Datos. En el Encabezado se incluye la dirección física del origen y del destino.

En el caso de IP se envían *Datagramas*, estos también incluyen un Encabezado y Datos, pero las direcciones empleadas son *Direcciones IP*.

Figura 3. Modelo general del datagrama IP

Autor.

[2] Aparte del Documento Resumen de IP Móvil, de la Facultad de Ciencias Físico Matemáticas de IANL. [Documento en Línea]. 2004. Disponible en Internet < http://ianl.es/equipo3.pdf >

Formato del Datagrama IP: los Datagramas IP están formados por *Palabras* de 32 bits. Cada Datagrama tiene un mínimo (y tamaño más frecuente) de cinco palabras y un máximo de quince, tal como se muestra en la figura 4.

Figura 4. Formato del datagrama IP

Ver	Hlen	TOS	Longitud Total	
Identificación			Flags	Desp. De Fragmento
TTL		Protocolo	Checksum	
Dirección IP de la Fuente				
Dirección IP del Destino				
Opciones IP (Opcional)				Relleno
DATOS				

Autor.

Se transmite en orden big endian: de izquierda a derecha, comenzando por el bit de orden mayor del campo de versión. (SPARC es big endian; Pentium es little endian). En las máquinas little endian, se requiere conversión por software tanto para la transmisión como para la recepción.

- Ver: versión de IP que se emplea para construir el Datagrama. Se requiere para que quien lo reciba lo interprete correctamente. La actual versión IP es la 4. El campo de versión lleva el registro de la versión del protocolo al que pertenece el datagrama. Al incluir la versión en cada datagrama es posible hacer que la transición entre versiones se lleve meses, o inclusive años, ejecutando algunas máquinas la versión antigua y otras la versión nueva.

- Hlen: tamaño de la cabecera en palabras. Dado que la longitud de la cabecera no es constante, se incluye un campo en la misma, IHL, para indicar la longitud en palabras de 32 bits. El valor mínimo es de 5, cifra que aplica cuando no hay opciones. El valor máximo de este campo de 4 bits es de 15, lo que limita la cabecera a 60 bytes y, por tanto, el campo de opciones a 40 bytes. Para algunas opciones, por ejemplo para una que registre la ruta que ha seguido un paquete, 40 bytes es muy poco, lo que hace inútil esta opción.

- TOS: tipo de servicio. La gran mayoría de los Host y Routers ignoran este campo. Su estructura es la que se muestra en la figura 5:

Figura 5. Campo tipo de servicio

Prioridad	D	T	R	Sin Uso

Autor.

La prioridad (0 = Normal, 7 = Control de red) permite implementar algoritmos de control de congestión más eficientes. Los tipos D, T y R solicitan un tipo de transporte dado: D = Procesamiento con retardos cortos, T = Alto Desempeño y R = Alta confiabilidad. Nótese que estos bits son solo "sugerencias", no es obligatorio para la red cumplirlo. El campo de tipo de servicio permite al host indicar a la subred el tipo de servicio que quiere. Son posibles varias combinaciones de confiabilidad y velocidad como ya se mencionó. Para voz digitalizada, la entrega rápida le gana a la entrega precisa o confiable.

- Longitud Total: la longitud total incluye todo el datagrama, es decir que mide en bytes la longitud de todo el Datagrama. Permite calcular el tamaño del campo de datos: datos = Longitud Total – 4 * Hlen.

Antes de continuar con la segunda palabra del Datagrama IP, es necesario introducir conceptos relacionados con la fragmentación.

Fragmentación: en primer lugar, De qué tamaño es un Datagrama? El tamaño para un Datagrama debe ser tal que permita la ***encapsulación***, esto es, enviar un Datagrama completo en una trama física. El problema está en que el Datagrama debe transitar por diferentes redes físicas, con diferentes tecnologías y diferentes capacidades de transferencia. A la capacidad máxima de transferencia de datos de una red física se le llama ***MTU*** o Maximum Transfer Unit (el MTU de Ethernet es 1500 bytes por trama, la de FDDI es 4497 bytes por trama). Cuando un Datagrama pasa de una red a otra con un MTU menor a su tamaño es necesaria la ***fragmentación***. A las diferentes partes de un Datagrama se les llama ***fragmento.*** Y al proceso de reconstrucción del Datagrama a partir de sus fragmentos se le llama ***Reensamblado de fragmentos***.
El control de la fragmentación de un Datagrama IP se realiza con los campos de la segunda palabra de su cabecera:

- Identificación: es un número de 16 bits que identifica al Datagrama, el cual permite implementar números de secuencias y que permite reconocer los diferentes fragmentos de un mismo Datagrama, pues todos ellos comparten este número. Este campo de identificación es necesario para que el host de destino determine a qué datagrama pertenece un fragmento recién llegado.

- Banderas: es un campo de tres bits donde el primero es un bit sin uso que está reservado. El segundo, llamado bit de No – Fragmentación significa: 0 = Puede fragmentarse el Datagrama o 1 = No puede fragmentarse el Datagrama. El tercer bit es llamado Más – Fragmentos y significa: 0 = Único fragmento o Último fragmento, 1 = aún hay más fragmentos. Cuando hay un 0 en Más – fragmentos, debe evaluarse el campo Desplazamiento de Fragmento (Desp. De fragmento): si este es cero, el Datagrama no está fragmentado, si es diferente de cero, el Datagrama es un último fragmento.

- Desplazamiento de Fragmento: a un trozo de datos se le llama Bloque de Fragmento. Este campo indica el tamaño del desplazamiento en bloques de fragmento con respecto al Datagrama original, empezando por el cero, es decir, en qué parte del datagrama actual va este fragmento.

Para finalizar con el tema de fragmentación, hay que mencionar el ***Plazo de Reensamblado***, que es un time out que el Host destino establece como máximo para esperar por todos los fragmentos de un Datagrama. Si se vence y aún no llegan TODOS, entonces se descartan los que ya han llegado y se solicita el reenvío del Datagrama completo.

- TTL: el campo de Tiempo de Vida del Datagrama, es un contador que especifica el número de segundos que se permite al Datagrama circular por la red antes de ser descartado, limitando la vida de un paquete.

- Protocolo: especifica que protocolo de alto nivel se empleó para construir el mensaje transportado en el campo datos del Datagrama IP. Algunos valores posibles son: 1 = ICMP, 6 = TCP, 17 = UDP, 88 = IGRP (Protocolo de Enrutamiento de Pasarela Interior de CISCO).

- Checksum: es un campo de 16 bits que se calcula haciendo el complemento a uno de cada palabra de 16 bits del encabezado, sumándolas y haciendo su complemento a uno. Esta suma hay que recalcularla en cada nodo intermedio debido a cambios en el campo de Tiempo de Vida o TTL (Time To Live en inglés) o por fragmentación.

- Dirección IP de la Fuente: la dirección de origen indica el número de red y el número de host de origen.

- Dirección IP del Destino: la dirección de destino indica el número de red y el número de host de destino.

- Opciones IP: existen hasta 40 bytes extra en la cabecera del Datagrama IP que pueden llevar una o más opciones. El campo de opciones se diseñó para proporcionar un recurso que permitiera que las versiones subsiguientes del protocolo incluyeran información no presente en el diseño original, para permitir a los experimentadores probar ideas nuevas y para evitar la asignación de bits de cabecera a información pocas veces necesaria. Las opciones son de longitud variable. Su uso es bastante raro. Algunas de las opciones son:

    - Uso de Ruta Estricta (Camino Obligatorio)
    - Ruta de Origen Desconectada (Nodos Obligatorios)
    - Crear Registro de Ruta
    - Marcas de Tiempo
    - Seguridad Básica del Departamento de Defensa
    - Seguridad Extendida del Departamento de Defensa

Enrutamiento IP: enrutar es el proceso de selección de un camino para el envío de paquetes. El computador o equipo que hace esto se denomina Router o Enrutador.

En general se puede dividir el enrutamiento en ***Entrega Directa*** y ***Entrega Indirecta***. La Entrega Directa es la transmisión de un Datagrama de una máquina a otra, dentro de la misma red física. La Entrega Indirecta ocurre cuando el destino no esta en la red local, lo que obliga al Host a enviar el Datagrama a algún Router intermedio. Es necesario el uso de máscaras de subred para saber si el Host de destino de un Datagrama está o no dentro de la misma red física.

Encaminamiento con Salto al Siguiente: la forma más común de enrutamiento requiere el uso de una ***Tabla de Enrutamiento IP***, presente tanto en los Host como en los Routers. Estas tablas no pueden tener información sobre cada posible destino, de hecho, esto no es deseable. En lugar de ello se aprovecha el esquema de direccionamiento IP para ocultar detalles acerca de los Host individuales, además, las tablas no contienen rutas completas, sino solo la dirección del siguiente paso en esa ruta.

En general una tabla de encaminamiento IP tiene pares (Destino, Router), donde destino es la dirección IP de un destino particular y Router la dirección del siguiente Router en el camino hacia destino. Nótese que el Router debe ser accesible directamente desde la máquina actual.

Este tipo de encaminamiento trae varias consecuencias, consecuencia directa de su naturaleza estática:

- Todo tráfico hacia una red particular toma el mismo camino, desaprovechando caminos alternativos y el tipo de tráfico.
- Solo el Router con conexión directa al destino sabe si este existe o está activo.
- Es necesario que los Routers cooperen para hacer posible la comunicación bidireccional.

1.4 ALGORITMO DE ENRUTAMIENTO IP

El procedimiento normal o lógico mediante el cual se encaminan los paquetes o datagramas desde un nodo de origen hasta un nodo de destino esta dado por el siguiente algoritmo de enrutamiento, el cual aplica la misma lógica de manera similar para el protocolo IP Móvil.

Ruta Datagrama (Datagrama) {
Extrae de la Cabecera de Datagrama la dirección de destino D;
Extrae de D el prefijo de Red N;
Si N corresponde a cualquier dirección directamente conectada **Entonces**
Envía el Datagrama a D sobre la Red N;
Sino
Si en la tabla hay una ruta especifica para D **Entonces**
Envía Datagrama al salto siguiente especificado;
Sino
Si En la tabla hay una ruta para la red N **Entonces**
Envía Datagrama al salto siguiente especificado;
Sino
Si En la tabla hay una ruta por defecto **Entonces**
Envía el Datagrama a la dirección por defecto;
Sino
Declarar Fallo de Enrutamiento;
Fsi
Fsi
Fsi
Fsi
}

Manejo de Datagramas Entrantes: cuando un Datagrama llega a un Host, el software de red lo entrega a IP. IP verifica la dirección de destino y si esta

concuerda con la de la máquina local, entonces acepta el Datagrama y lo entrega a las capas superiores. De no coincidir la dirección de destino, el Datagrama es descartado.

Por otra parte, un Router que reciba un Datagrama compara la dirección de destino con la suya propia. Si coinciden, el Datagrama pasa a las capas superiores, sino, se le aplica el algoritmo de encaminamiento y se reenvía el Datagrama.

Direccionamiento sin Clase: muchas veces se ha explicado respecto a TCP/IP como mediante el empleo de Mascaras de subred, se logra convertir una única red (generalmente una Clase B) en múltiples redes lógicas interconectadas y administradas por la organización propietaria. El problema se presenta cuando el crecimiento explosivo de las redes locales produce el fenómeno ROADS (Running Out of Address Space), que consiste simplemente en el agotamiento del espacio de direcciones útil, causado por la gran demanda de las direcciones Clase B, de las cuales solo hay 16.384, mientras que las Clases C permanecían sin Asignar (pues aunque hay 2.097.152 de ellas, nadie las quiere por ser muy pequeñas).

Para enfrentar este problema se desarrollo el esquema de Direcciones sin Clase, que consiste en asignar a una misma organización un bloque continuo de direcciones de Clase C. De esta manera, una organización que requiera conectar a Internet un número moderado de Hosts (por ejemplo 3.800) puede recibir un bloque de 16 redes continuas de Clase C (por ejemplo, de la red Clase C 199.40.72.0 a la 199.40.87.0), con lo cual dispone de 4.096 direcciones IP validas para administrar.

CIDR Enrutamiento Inter – Dominio Sin Clases (Classless Inter – Domain Routing): el esquema de direcciones sin clase genera el problema de aumentar la información que debe incluirse en las tablas de enrutamiento. En el caso del ejemplo, se tendrían que incluir 16 nuevas entradas en cada tabla de enrutamiento de cada Host y Router. CIDR resuelve el problema al incluir en las tablas información acerca del tamaño de los bloques y el número de bloques, así, en las tablas de enrutamiento IP se tienen pares (Destino, Router), donde el destino no es una dirección de Host o Red tradicional, sino que incluye información acerca del número de redes que incluye el bloque (en el ejemplo, 16) y el tamaño de cada una de esas redes (en el ejemplo, son Clases C, 256 direcciones cada una).

El Direccionamiento sin clase modifica la estructura de una dirección IP, como se muestra en la figura 6:

Figura 6. Campos del direccionamiento sin clase

Autor.

Así, CIDR debe incluir en las tablas de enrutamiento cual es la primera red que compone el bloque, cuantos bits se emplean como Prefijo de Red y la máscara de subred que se emplea. En nuestro ejemplo, las tablas de enrutamiento IP contendrían esta información:

199.40.72.0/20 255.255.240.0

Refiriéndose a un bloque que se inicia con la red 199.40.72.0 y que tiene 20 bits en el prefijo de red. La mascara 255.255.240.0 (11111111.11111111.1111***0000***.00000000) nos indica que se están usando 4 bits extra (los resaltados) para identificar a las redes que componen al bloque. Nótese que cuatro bits permiten agrupar precisamente 16 redes Clase C.

Un aspecto importante que hay que subrayar es que en ningún momento cambia el algoritmo básico de enrutamiento IP, lo que cambia es el contenido de las tablas. Además, las nuevas tablas contienen información resumida, por lo que buscar una dirección destino en la tabla se hace de otra manera, pero el algoritmo permanece inalterado.

El problema de buscar direcciones de destino en una tabla, consiste en que cualquier dirección cuya máscara de destino tenga menos bits, incluye a la que tiene más bits. Lo que se quiere decir con esto es que una máscara de subred como 255.255.0.0 (***11111111.11111111***.00000000.00000000, es decir, 16 bits de prefijo de red) incluye dentro de si a la máscaras de subred 255.255.128.0 (***11111111.11111111.1***0000000.00000000, 17 bits de prefijo de red) y esta a su ves incluye a la máscara 255.255.192.0 (***11111111.11111111.11***000000.00000000) y en general, entre menos bits tiene el prefijo de red, más direcciones Host abarca. Por esta razón cuando se explora la tabla de enrutamiento IP en busca de una dirección de destino, se hace una búsqueda que inicia con las máscaras de más bits y termina en la de menos bits. Es decir, se inicia con máscaras como 255.255.255.255 (todo en uno) y se continua con la 255.255.255.254 (31 unos y un cero) y así sucesivamente. Esto quiere decir que tendrían que hacerse 32 recorridos secuenciales a la tabla, lo cual es muy ineficiente en cuanto a tiempo, pues además de ser un procedimiento demorado, se sabe ya que direcciones normales de Clase B (255.255.0.0) requieren 16 barridos a la tabla, además, hacen falta 32 barridos para notar que no hay una entrada en la tabla para esas direcciones. Por esta razón se emplean otros métodos para hacer estas búsquedas en las tablas de enrutamiento IP. Un esquema muy popular emplea un Árbol Binario, en el cual cada bit representa una nueva rama en el árbol.

Así, en el ejemplo, podrían dividirse las direcciones asignadas a la organización (4.096) en subredes de esta forma: dos subredes de 1.024 direcciones cada una, tres de 512 y dos de 256 direcciones.

ICMP, Protocolo de Mensajes de Control de Internet (Internet Control Message Protocol): si un Router no puede enrutar o entregar un Datagrama, o si detecta una situación anómala que afecta su capacidad de hacerlo (por ejemplo, la congestión), debe informar a la fuente original para que evite o solucione el problema.

ICMP es un mecanismo para realizar esta operación. Es considerado como una parte obligatoria de IP y debe ser incluido en todas sus implementaciones. ICMP comunica la capa de Internet de una máquina con la misma capa en otra máquina. ICMP es un protocolo de ***reporte de errores*** (no los corrige), además, ICMP solo puede informar del error a la fuente del Datagrama; es esta máquina la que debe implementar mecanismos para enfrentar el problema.

Los mensajes de ICMP requieren doble encapsulación: los mensajes ICMP viajan empaquetados en Datagramas IP. Aun así, no se considera a ICMP un protocolo de nivel superior a IP.

Formato del Mensaje ICMP: aunque cada tipo de mensaje tiene su propio formato, todos ellos comparten los primeros tres campos: TIPO (8 bits), CODIGO (8 bits) y CHECKSUM (16 bits), como se puede ver en la figura 7.

El campo TIPO identifica al tipo de mensaje ICMP y determina su formato. Puede tener alguno de estos valores:

- 0 : Respuesta de Eco (Echo Replay)
- 3 : Destino Inaccesible (Host Unreachable)
- 4 : Acallamiento de Origen (Source Quench)
- 5 : Redireccionar (Redirect)
- 8 : Solicitud de Eco (Echo Request)
- 11 : Tiempo Excedido
- 12 : Problema de Parámetros
- 13 : Solicitud de Timestamp
- 14 : Respuesta de Timestamp
- 17 : Solicitud de máscara de subred
- 18 : Respuesta de máscara de subred

Mensajes Solicitud de Eco y Respuesta al Eco: este es el tipo de mensaje que envía la máquina cuando se emplea el comando ping. Solicitud de Eco pide a la maquina destino que responda con una Respuesta de Eco con un número de secuencia apropiado.

Figura 7. Formato de mensaje ICMP

TIPO (8 o 0)	CODIGO (0)	CHECKSUM
Identificador		Numero de Secuencia
Datos Opcionales		

Autor.

Mensaje Destino Inaccesible: es el mensaje empleado para reportar que no es posible entregar un Datagrama. Ver figura 8. El campo CODIGO describe mejor el problema:

- 0 : Red Inaccesible
- 1 : Host Inaccesible
- 2 : Protocolo Inaccesible
- 3 : Puerto Inaccesible
- 4 : Necesita Fragmentación
- 5 : Falla en la Ruta de Origen
- 6 : Red de Destino Desconocida
- 7 : Host Destino Desconocido
- 8 : Host de Origen Aislado
- 9 : Comunicación con Red Destino Administrativamente Prohibida
- 10 : Comunicación con Host Destino Administrativamente Prohibida
- 11 : Red Inaccesible por el tipo de servicio
- 12 : Host Inaccesible por el tipo de servicio

Figura 8. Mensaje destino inaccesible

TIPO (3)	CODIGO (0...12)	CHECKSUM
NO – USADO (debe ser cero)		
Encabezado IP + Primeros 8 bytes de Datos IP		

Autor.

Los errores de red inaccesible por lo general implican fallas de enrutamiento. Debido a que el mensaje ICMP contiene la cabecera del Datagrama que lo produjo (en el campo de datos), el origen sabrá cual destino es inaccesible.

Mensaje de Acallamiento de Origen: debido a que IP funciona sin conexión un Router no puede reservar memoria o recursos de comunicación antes de recibir los Datagramas. En consecuencia los Routers pueden verse repentinamente saturados por el trafico. A esta situación se le llama congestión.

El congestionamiento se da porque un Host de alta velocidad genera Datagramas más rápido de lo que el Router puede manejar o porque muchos Hosts envían Datagramas a la misma dirección al mismo tiempo.

Cuando los Datagramas llegan más rápido de lo que un Router puede manejarlos, este los coloca en un buffer. Si los Datagramas son parte de una ráfaga pequeña, esto soluciona el problema, pero si continúan llegando Datagramas se saturan los buffers y el Router debe descartar los nuevos Datagramas. Es entonces cuando el Router genera un mensaje ICMP de Acallamiento de Origen solicitando a este reducir la tasa de envío de Datagramas, tal como se muestra en la figura 9. No existe un mensaje ICMP para revertir esta solicitud, en general poco después de bajar la tasa de envío, los Hosts la aumentan progresivamente hasta recibir otro mensaje de Acallamiento de Origen.

Figura 9. Mensaje de acallamiento de origen

TIPO (4)	CODIGO (0)	CHECKSUM
NO - UTILIZADO (debe ser cero)		
Encabezado IP + 8 primeros bytes de Datos IP		

Autor.

El objetivo de este mensaje era aliviar el problema de la congestión, pero no tuvo éxito. Se dejo a quien lo implementa decidir sobre cuando enviar estos mensajes, por lo que cada fabricante emplea su política favorita sin que ninguna solucione el problema del todo. Por otra parte, ICMP informa al Host de origen que su Datagrama ha sido descartado, pero puede que este Host no sea el causante de la congestión. Además, Cómo responder al mensaje ICMP? Documentos como ***Requisitos para los Routers*** (RFC 1812) estipulan que NO se deben enviar mensajes de Acallamiento de Origen. Se está trabajando en mecanismos más eficientes.

Mensaje Redireccionar: se asume que los Routers conocen rutas correctas. Los Hosts comienzan con información mínima de enrutamiento y aprenden nuevas rutas de los Routers. En caso de que un Host utilice una ruta no óptima, el Router que lo detecta envía un mensaje ICMP Redireccionar como el que se observa en la figura 10, solicitándole que actualice su tabla de enrutamiento IP.

Figura 10. Mensaje redireccionar

TIPO (5)	CODIGO (0...3)	CHECKSUM
Dirección IP del Router		
Encabezado de IP + 8 primeros bytes de Datos IP		

Autor.

Mensaje Tiempo Excedido: debido a que los Routers solo deciden sobre el próximo "Salto" usando tablas locales, errores en esas tablas pueden generar "ciclos de enrutamiento" para algún destino. Esto provoca que los Datagramas sean descartados por vencimiento de su TTL. Siempre que un Router descarte un Datagrama ya sea por vencimiento de TTL o por vencimiento del Tiempo de Reensamblado, envía un mensaje de Tiempo Excedido a la fuente, como el de la figura 11.

Figura 11. Mensaje tiempo excedido

TIPO (11)	CODIGO (0 o 1)	CHECKSUM
NO – UTILIZADO (debe ser cero)		
Encabezado de IP + 8 primeros bytes de Datos IP		

Autor.

CODIGO = 0: Descartado por vencimiento de TTL
CODIGO = 1: Descartado por vencimiento de Tiempo de Reensamblado.

Mensaje Problema de Parámetros: cuando un Router o un Host encuentra un problema que no ha sido cubierto con los mensajes ICMP anteriores, envía este mensaje, que se muestra en la figura 12.

Figura 12. Mensaje problema de parámetros

TIPO (12)	CODIGO (0 o 1)	CHECKSUM
Indicador	NO – Utilizado (debe ser cero)	
Encabezado de IP + 8 primeros bytes de Datos IP		

Autor.

El campo indicador apunta al campo dentro del encabezado IP que generó el problema.

Mensaje Solicitud de Timestamp y Respuesta de Timestamp: una técnica sencilla provista por TCP/IP para sincronizar relojes emplea ICMP para obtener

la hora de la otra máquina. Una máquina envía a otra una solicitud de Timestamp, solicitándole que informe su valor actual para la hora del día, con un mensaje como el que se muestra en la figura 13. La otra máquina envía una respuesta de Timestamp con esa información.

Figura 13. Mensaje solicitud de timestamp y respuesta de timestamp

TIPO (13 o 14)	CODIGO (0)	CHECKSUM
Identificador		Numero de Secuencia
Timestamp Origen		
Timestamp al Recibir		
Timestamp al Transmitir		

Autor.

Mensaje Solicitud de Máscara de Subred y Respuesta de Máscara de Subred: para aprender la máscara de subred utilizada por la red local, una máquina puede enviar un mensaje ICMP Solicitud de Máscara de Subred como el observado en la figura 14, a un Router y esperar su Respuesta. Si la máquina no conoce la dirección del Router, puede enviar este mensaje por difusión.

Figura 14. Mensaje solicitud de máscara de subred y respuesta de máscara de subred

TIPO (17 o 18)	CODIGO (0)	CHECKSUM
Identificador		Numero de Secuencia
Mascara de Subred		

Autor.

1.5 ESTADO DEL ARTE

El protocolo IP existente hoy en día esta siendo modificado para ofrecer movilidad y acceso global a los usuarios Internet, a través de la IETF (Internet Engineering Task Force) y sus RFC's relacionados con el tema y a través de algunas de las empresas más importantes del mercado de las comunicaciones en el ámbito mundial. Además alrededor del mundo se han realizado algunos estudios sobre el tema desde diferentes puntos de vista, incluso en Colombia.

Actualmente están siendo propuestos cuatro protocolos IP Móvil o Mobile-IP que se diferencian en sus características internas y los cuales están en proceso de perfeccionamiento; estos son:

- Mobile-IP: de la Universidad de Columbia en los Estados Unidos.
- Mobile-IP IBM I: desarrollado por la empresa IBM en los Estados Unidos.
- Mobile-IP VIP: de la empresa Sony del Japón, llamado Mobile IP - VIP (virtual Internet Protocol) o VIPon V6 (Virtual Internet Protocol on version 6 IP)
- Mobile-IP IBM II: desarrollado por la empresa IBM en los Estados Unidos.

La especificación de un protocolo Mobile-IP genérico esta siendo realizada conjuntamente con la especificación de las futuras generaciones de los protocolos IP y cuya capacidad de direccionamiento es muy superior a la actual. Adicionalmente permite direccionamientos del tipo Single, Anycast y Multicast. Todo esto ha sido y está siendo estudiado por la IETF (Internet Engineering Task Force).

Para eliminar el problema de compatibilidad, la IEFT establece mecanismos que aseguran la compatibilidad dentro de la red, cualquiera sea el protocolo IP (IPv4 o IPv6).

Por otro lado, además de los estudios netamente científicos y profesionales, a lo largo del mundo se han desarrollado otros estudios de tipo un poco más informal, que tratan el tema de IP Móvil dentro del ámbito de las aplicaciones, servicios, comparaciones con otras tecnologías, y análisis de la migración a esta tecnología en el mercado.

Algunos de los estudios más representativos son:

- Universidad de Bremen, Alemania: crearon un sitio Web llamado Mobile IP.org dedicado a la discusión y publicación de software abierto, white papers, estándares propuestos y otras noticias de investigación en el área del soporte de la movilidad de Internet. Algunos de los temas de investigación relacionados con IP Móvil son:

    - Plataformas de red integradas basadas en Internet Móvil y en protocolo multi-hop y ad hoc.
    - Evaluación y optimización del rendimiento de protocolos de Internet Móvil, por medio de análisis teórico, simulaciones y prototipos.
    - Determinación del impacto de overhead de protocolos IP Móvil en un rango de aplicaciones IP y en la World Wide Web.
    - Incremento del rendimiento de IP Móvil mediante la eliminación o reducción de overheads, integración de tecnologías inalámbricas heterogéneas y el perfeccionamiento de los terminales móviles.

- Universidad Nacional de Colombia, Colombia: el único estudio tal vez publicado o que se sepa en Colombia el cual trata de un trabajo de tesis de maestría que actualmente esta siendo desarrollado, por Luis Guillermo Martínez Ballesteros. Es un estudio y análisis de la transferencia de tecnología requerida hacia IP Móvil en redes de comunicación personalizada (PCS) a nivel de señalización y enrutamiento.

- Universidad Santo Tomás, Colombia: a la fecha no se han encontrado estudios que se hayan hecho en la universidad. El presente trabajo hace parte del primer estudio a nivel de investigación y definición del protocolo IP Móvil, a manera de descripción general y profunda.

- Universidad de Macquire, Australia: varios estudios desarrollados por A. Myles y David Skellern, de la escuela de Matemáticas, Física, Computación y Electrónica. Algunos de los temas tratados son:

  - Comparación de protocolos de Host móvil para IP (1.993).
  - Análisis de seguridad y privacidad en IP Móvil (1.996).
  - Soporte de red para host móviles en una interconexión de red TCP/IP (1.995).
  - The Internet Mobile Host Protocol (IMHP).
  - Comparando 4 Protocolos de Host Móvil basados en IP.
  - Soporte Multicast para host móviles usando IP Móvil (1.999).

- Academia Sinica, China: proyecto de una plataforma de red que provea servicios de movilidad en Internet con características de alto rendimiento, facilidad de uso y aseguramiento; técnicas para mejorar el enrutamiento y la eficiencia de handoff en IP Móvil, incluyendo soporte de la optimización de rutas bi-direccionales simétricas, y reducción de la pérdida de paquetes. El objetivo es darle al cliente, técnicas para que utilice las ventajas de IP Móvil con dispositivos existentes y que no requieran actualizaciones software, como de Sistemas Operativos u otros elementos de hardware.

2. INTRODUCCIÓN A IP MÓVIL

La versión 4 de IP (Ipv4) asume que la dirección IP de un nodo únicamente identifica el punto de conexión del nodo a Internet. Por lo tanto, un nodo debe ser localizado en la red indicada por medio de su dirección IP, con el objeto de recibir los datagramas destinados a él; de lo contrario, los datagramas destinados al nodo no serán entregables. Para que un nodo pueda cambiar su punto de conexión sin perder su habilidad de comunicación, normalmente debe emplear uno de los siguientes dos mecanismos típicos:

- El nodo debe cambiar su dirección IP, en el momento que cambie su punto de conexión.
- Se deben propagar Rutas específicas de host a través de la mayor parte de la estructura de enrutamiento de Internet.

Ambas alternativas son a menudo inaceptables. La primera hace imposible mantener las conexiones de la capa de transporte y de la capa más alta, para un nodo, cuando éste cambia de localización. La segunda tiene problemas de escalamiento obvios y severos, especialmente relevantes, considerando el crecimiento tan acelerado y explosivo de computadores portátiles (Notebooks y Laptops).

Se requiere entonces un nuevo mecanismo escalable para acomodar la movilidad del nodo a Internet. En los capítulos siguientes del trabajo se pretende definir tal mecanismo, el cual habilita a los nodos para cambiar su punto de conexión a Internet sin cambiar su dirección IP.

Es necesario aclarar que aún esta tecnología no ha sido desarrollada por completo y por tal motivo, es probable que hayan surgido cambios en cualquier momento los cuales no estén incluidos al momento de revisar este trabajo acerca del Protocolo IP Móvil, por motivos de tiempos y actualización inmediata de la información. Sin embargo, se tratan de explicar lo más detallado posible todas las características y las especificaciones más recientes.

2.1 REQUERIMIENTOS DEL PROTOCOLO

Un nodo móvil debe ser capaz de comunicarse con otros nodos después de cambiar su punto de conexión de capa de enlace a Internet, aún sin cambiar su dirección IP.

Un nodo móvil debe ser capaz de comunicarse con otros nodos que no implementan estas funciones de movilidad. Además no se requieren mejoras en hosts o routers que no están actuando como alguna de las nuevas entidades de la arquitectura de IP Móvil, las cuales se describen más adelante.

Todos los mensajes utilizados para actualizar otro nodo, como la localización de un nodo móvil, deben ser autenticados con el objeto de protegerlo contra ataques de redireccionamiento remotos.

2.2 METAS

El enlace por el cual un nodo móvil está directamente conectado a Internet debe ser a menudo un enlace Wireless o inalámbrico. Este enlace debe entonces tener substancialmente ancho de banda más bajo y mayor tasa de errores que las redes alámbricas tradicionales. Además, es probable que los nodos móviles sean de baterías (es el caso de computadores portátiles y agendas personales), y minimizar el consumo de potencia es importante. Por lo tanto, el número de mensajes administrativos enviados sobre el enlace por el cual un nodo móvil está directamente conectado a Internet debe ser minimizado y el tamaño de estos mensajes debe mantenerse tan pequeño como sea posible.

2.3 SUPOSICIONES

Los protocolos que se mencionan a lo largo del trabajo no ponen restricciones adicionales en la asignación de direcciones IP. Esto es, a un nodo móvil se le puede asignar una dirección IP a través de la organización que posee la máquina.

El Protocolo IP Móvil asume que los nodos móviles generalmente no cambiarán su punto de conexión a Internet, con una frecuencia mayor a una vez por segundo.

Además este protocolo asume que los datagramas IP unicast son enrutados, basándose en la dirección de destino en la cabecera del datagrama (y no, por ejemplo, por la dirección de origen).

2.4 APLICABILIDAD

IP Móvil pretende habilitar nodos para moverlos desde una subnet a otra. Esto es tan adecuado tanto para movilidad a través de medios homogéneos, como para movilidad a través de medios heterogéneos. Esto quiere decir que IP Móvil facilita el movimiento del nodo desde un segmento Ethernet a otro; de igual manera, también acomoda el movimiento de nodos desde un segmento Ethernet a una LAN inalámbrica o Wireless LAN, por tanto tiempo como el nodo móvil mantenga la misma dirección IP, después haber realizado tal movimiento.

Se puede pensar en IP Móvil como la solución al problema de administración de “macro” movilidad. La razón de ello es que este protocolo es menos apropiado para mayor cantidad de aplicaciones de administración de “micro” movilidad, como por ejemplo, handoff entre transceptores inalámbricos, de los cuales cada uno cubre solo una pequeña área geográfica. A medida que el movimiento del nodo no ocurra entre puntos de conexión en diferentes subredes IP, los mecanismos para movilidad de capa de enlace (handoff de capa de enlace) pueden ofrecer convergencia más rápida y mucho menos overhead que IP Móvil.

2.5 NUEVAS ENTIDADES DE LA ARQUITECTURA

IP Móvil introduce nuevas entidades funcionales para su correcta operación. Las entidades principales son las siguientes:

- Nodo móvil: es un host (computador portátil, agenda personal, etc.) o un router que cambia su punto de conexión habitual de una red o subred a otra. Un nodo móvil puede cambiar su localización sin cambiar su dirección IP; puede continuar comunicándose con otros nodos de Internet en cualquier ubicación usando su dirección IP (constante), asumiendo que la conectividad de capa de enlace a un punto de conexión, está disponible.

- Agente local: es un router sobre la red local del nodo móvil el cual envía los datagramas a través de un túnel (este proceso se conoce como Tunneling) para entregar al nodo móvil, cuando éste último está lejos de su sitio local y mantiene información de la localización actual para el nodo móvil.

- Agente externo: es un router sobre una red visitada (red externa diferente de la red local) por el nodo móvil, el cual provee servicios de enrutamiento al nodo móvil mientras esté registrado en aquella red. El agente externo hace el proceso contrario de envío a través de un túnel (Tunneling), es decir saca del túnel y entrega al nodo móvil los datagramas que fueron encapsulados en el túnel por el agente local del nodo móvil. Para los datagramas que son enviados por un nodo móvil, el agente externo puede servir como un router por defecto para los nodos móviles registrados en la red externa.

Un nodo móvil ha sido creado para tener una dirección IP de término largo (durante mucho tiempo) en una red local. Esta dirección local es administrada de la misma forma en que una dirección IP "permanente" es dada a un host estacionario (por ejemplo un computador de escritorio). Cuando se está lejos de la red local, una "dirección temporal" (Care-off address) está asociada con el nodo móvil y refleja el punto actual de conexión del nodo móvil. El nodo móvil además, utiliza su dirección local como la dirección de origen de todos los datagramas IP que envía, excepto para datagramas enviados para ciertas funciones de administración de movilidad.

2.6 TERMINOLOGÍA

Algunas de las palabras que tienen que ver con el desarrollo del Protocolo IP Móvil y su significado pueden ser consultadas de manera más detallada en el RFC 2119 donde se describe su interpretación. Por otro lado, es importante resaltar que se han escogido algunos términos clave que son utilizados de manera frecuente a lo largo de este trabajo y por esto su definición más completa se describe a continuación:

- Extensión de habilitación de autorización: es una autenticación la cual hace que un mensaje (Registro) sea aceptable para el último receptor del mensaje de registro. Una extensión de habilitación de autorización debe contener un SPI (Índice de Parámetros de Seguridad).

Todos los usos de la extensión de habilitación de autorización se refieren a las extensiones de autenticación que habilitan que el mensaje de solicitud de registro, sea aceptable para el agente local. Utilizando estructuras de protocolo adicionales especificas, las cuales están por fuera de este documento, puede hacerse posible que el nodo móvil provea autenticación de su registro al agente local, por medio de otra entidad de autenticación dentro de la red, que sea aceptable para el agente local (RFC 2794).

- Aviso del agente: es un mensaje de aviso construido mediante la conexión de una extensión especial, a un mensaje de aviso de router.

- Autenticación: es el proceso de verificación (usando técnicas criptográficas, para todas las aplicaciones de este protocolo) de identidad, del que origina el mensaje.

- Dirección temporal (Care-off address): consiste en el punto final de un túnel hacia un nodo móvil, para datagramas remitidos al nodo móvil, mientras este está lejos de su sitio local (Tunneling). El protocolo puede usar dos (2) diferentes tipos de dirección temporal (Care-off address): “una dirección temporal del agente externo” la cual es una dirección de un agente externo con la cual el nodo móvil es registrado, y una “dirección temporal Co-Located” que es una dirección local obtenida externamente, la cual el nodo móvil tiene asociada con una de sus interfaces de red.

- Nodo correspondiente: es un extremo con el cual un nodo móvil está comunicándose. Un nodo correspondiente puede ser móvil o estacionario.

- Red foránea o red Externa: cualquier otra red diferente de la red local del nodo móvil; es decir, cualquier red diferente de la red a la cual el nodo móvil está conectado habitualmente.

- ARP (Addres Resolution Protocol) gratuito: es un paquete ARP enviado por un nodo con el objetivo de causar espontáneamente que otros nodos se actualicen y entren en su ARP caché.

- Dirección local: es una dirección IP que es asignada durante un periodo de tiempo extendido para un nodo móvil. Esta se mantiene intacta a pesar del sitio donde el nodo se encuentre conectado a Internet.

- Red local: es una red, posiblemente virtual, la cual posee un prefijo que se ajusta a aquella dirección local de un nodo móvil. Se debe tener en cuenta que los mecanismos estándar de enrutamiento IP entregarán los datagramas destinados a la dirección local del nodo móvil, justamente a la red local del nodo móvil.

- Enlace: es una facilidad (Capa de Enlace del Modelo OSI) o medio sobre el cual los nodos pueden comunicarse en la capa de enlace. Un enlace es la base de la capa de red.

- Dirección de capa de enlace: son las direcciones utilizadas para identificar un punto final de algunas comunicaciones sobre un enlace físico. Típicamente, la dirección de capa de enlace es una dirección de control de acceso al medio (MAC por sus siglas en inglés) de la interfaz.

- Agente móvil: puede ser cualquiera de los dos: un agente local o un agente externo.

- Vínculo de movilidad: es la asociación de una dirección local con una dirección temporal, junto con el tiempo de vida que permanece esa asociación.

- Asociación de seguridad de movilidad: consiste en una colección de contextos de seguridad entre un par de nodos, los cuales pueden ser aplicados a los mensajes del protocolo IP Móvil intercambiados entre ellos. Cada contexto indica un algoritmo de autenticación y un modo de autenticación, un secreto (una clave compartida o unas llaves pública y privada adecuadas) y un estilo de protección de repetición en uso.

- Nodo: puede ser un host o un router.

- Nonce: es un valor escogido aleatoriamente, diferente de elecciones previas, insertado en un mensaje para proteger contra repeticiones.

- Índice de parámetros de seguridad (SPI): es un índice identificando un contexto de seguridad entre un par de nodos, entre los contextos disponibles en la asociación de seguridad de movilidad. Los valores del SPI desde cero (0) hasta 255 están reservados y NO deben ser usados en ninguna asociación de seguridad de movilidad.

- Túnel: es el camino seguido por un datagrama mientras éste es encapsulado. El modelo es que, mientras es encapsulado, un datagrama es enrutado hacia un agente desencapsulador erudito, el cual desencapsula el datagrama y entonces lo entrega correctamente a su último destino (Tunneling).

- Red virtual: es una red sin instalación física más allá de un router (con una interfaz de red física sobre otra red). El router (agente local) generalmente advierte el grado de rechazo a la red virtual, utilizando protocolos de enrutamiento convencionales.

- Red visitada: es una red cualquiera fuera de la red local del nodo móvil, a la cual el nodo móvil está actualmente conectado.

- Lista de visitantes: es la lista de nodos móviles que se encuentran visitando un agente externo.

2.7 VISION GENERAL DEL PROTOCOLO

Para IP móvil se encuentran definidos los siguientes servicios de soporte:

- Descubrimiento del agente: los agentes locales y los agentes externos pueden avisar su disponibilidad sobre cada enlace para el cual ellos proveen servicio. Un nodo móvil recién llegado puede enviar una solicitud sobre el enlace para ver si algunos agentes posibles se presentan.

- Registro: cuando el nodo móvil está lejos de su sitio local, éste registra su dirección temporal con su agente local. Dependiendo de su método de acople, el nodo móvil se registrará directamente con su agente local o a través de un agente externo, el cual remite el registro al agente local.

- Descarte silenciosamente: la implementación de IP Móvil, descarta el datagrama sin procesamiento adicional y sin indicar un error al remitente. La implementación además debería proveer la capacidad de registrar el error, incluyendo el contenido del datagrama descartado y debería grabar el evento en un contador de estadísticas.

Los siguientes pasos proveen un vago resumen de la operación del protocolo IP móvil:

- Los agentes de movilidad (por ejemplo agentes externos y agentes locales) advierten su presencia por medio de mensajes de aviso del agente. Un nodo móvil puede opcionalmente solicitar un mensaje de aviso del agente desde agentes de movilidad conectados localmente, a través de un mensaje de solicitud de agente.
- Un nodo móvil recibe estos avisos de agente y determina si está en su red local o en una red externa.
- Cuando un nodo móvil detecta que está localizado en su red local, éste opera sin servicios de movilidad. Si se regresa a su red local estando registrado desde cualquier parte, el nodo móvil se desregistra con su agente local, a través del intercambio de una solicitud de registro y un mensaje de respuesta de registro.
- Cuando un nodo móvil detecta que ha sido movido a una red externa, éste obtiene una dirección temporal sobre la red externa. La dirección temporal puede ser determinada a partir de avisos de agente externo (una dirección temporal de agente externo), o por medio de mecanismos de asignación externos como DHCP (una dirección temporal CO-located). El mecanismo DHCP o Protocolo de Configuración de Host Dinámico (Dynamic Host Configuration Protocol) asigna una dirección IP al nodo móvil de manera flexible y transparente para él.
- El nodo móvil operando lejos de su red local registra entonces su nueva dirección temporal con su agente local, a través del intercambio de una solicitud de registro y un mensaje de respuesta de registro con él, posiblemente por medio de un agente externo.
- Los datagramas enviados a la dirección local del nodo móvil son interceptados por su agente local, enviados a través de un túnel por el agente local hacia la dirección temporal del nodo móvil, recibidos al final del túnel (bien en un agente externo o en el mismo nodo móvil) y finalmente entregados al nodo móvil; este procedimiento se conoce como Tunneling.
- En sentido contrario, los datagramas enviados por el nodo móvil son entregados generalmente a su destino usando mecanismos convencionales de enrutamiento IP, sin pasar necesariamente a través del agente local.

Cuando se está lejos de casa, IP Móvil utiliza encapsulamiento con túneles para esconder una dirección local del nodo móvil desde los routers que intervienen entre su red local hasta su localización actual. El túnel termina en la dirección temporal del nodo móvil. La dirección temporal debe ser una dirección a la cual los datagramas pueden ser entregados por medio de enrutamiento IP convencional. En una dirección temporal, el datagrama original es removido del túnel y entregado al nodo móvil (Tunneling).

IP Móvil brinda dos modos alternativos para adquirir una dirección temporal:

- Una “dirección temporal de agente externo” es una dirección temporal dada por un agente externo, por medio de sus mensajes de Aviso de Agente. En este caso, la dirección temporal es una dirección IP de agente externo. De esta forma, el agente externo es el punto final del túnel y sobre el cual se reciben los datagramas encapsulados, los desencapsula y entrega el datagrama encapsulado al nodo móvil. Este método de adquisición es el más preferido porque permite a muchos nodos móviles compartir la misma dirección temporal y por lo tanto no implica demandas innecesarias, en el ya limitado espacio de direcciones IPv4.

- Una “dirección temporal Co-located” es una dirección temporal adquirida por el nodo móvil como una dirección IP local a través de algunos medios externos, la cual el nodo móvil asocia entonces con una de sus propias interfaces de red. La dirección puede ser adquirida dinámicamente como una dirección temporal por el nodo móvil a través de DHCP, o puede pertenecerle al nodo móvil como una dirección de largo-plazo para su uso únicamente mientras visita alguna red externa. Existen algunos métodos externos específicos de adquisición de una dirección IP local para usarla como una dirección temporal Co-located, los cuales no se describen aquí. Cuando se usa una dirección temporal Co-located, el nodo móvil sirve como el punto final del túnel y por si mismo ejecuta el desencapsulamiento de los datagramas encapsulados en el túnel hacia él.

El uso de una dirección temporal Co-located tiene la ventaja de que permite a un nodo móvil funcionar sin un agente externo, por ejemplo, en redes que no tienen todavía desarrollado un agente externo. Esto hace, sin embargo, que se coloque carga adicional en el espacio de direcciones IPv4 porque se requiere un conjunto de direcciones dentro de la red externa, para que esté disponible cuando haya la visita de nodos móviles. De esta forma, resulta difícil mantener eficientemente el grupo de direcciones para cada subnet, el cual puede permitir la visita de nodos móviles.

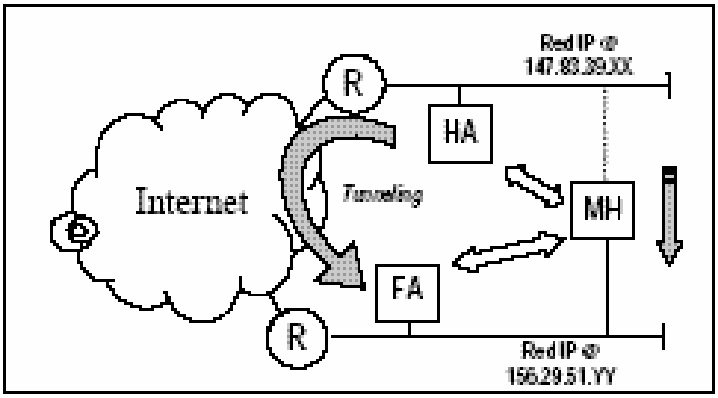
Es importante entender la diferencia entre la dirección temporal y las funciones del agente externo. La dirección temporal es simplemente el punto final del túnel. Ésta puede ser verdaderamente una dirección de un agente externo (una dirección temporal de agente externo), pero por el contrario puede ser una dirección temporalmente adquirida por el nodo móvil (una dirección temporal Co-located). Un agente externo, por su parte es un agente de movilidad que brinda servicios a nodos móviles.

Un agente local debe ser capaz de atraer e interceptar datagramas que están destinados a la dirección local de cualquiera de sus nodos móviles registrados.

Utilizando mecanismos Proxy y ARP gratuitos los cuales son descritos más adelante en la sección 5.6, se puede satisfacer este requerimiento, si el agente local tiene una interfaz de red en el enlace indicado por la dirección local del nodo móvil. Otras ubicaciones del agente local, relativas a la localización local del nodo móvil, también pueden ser posibles, utilizando otros mecanismos para interceptar datagramas, destinados a la dirección local del nodo móvil. Estas ubicaciones no se describen en este trabajo ya que implicaría salirse del tema principal, objeto del mismo.

De manera similar, un nodo móvil y un agente prospectivo o actual, debe ser capaz de intercambiar datagramas sin depender de mecanismos de enrutamiento IP estándares; esto es, aquellos mecanismos los cuales hacen seguimiento de decisiones, basados en el prefijo de red de la dirección de destino dentro del encabezado IP. Este requerimiento puede ser satisfecho si el agente externo y el nodo móvil visitante, tienen una interfaz en el mismo enlace. En este caso, el nodo móvil y el agente externo simplemente eluden sus mecanismos normales de enrutamiento IP, cuando se envían datagramas del uno al otro, direccionando los paquetes de capa de enlace hacia sus respectivas direcciones de capa de enlace. Otras ubicaciones del agente externo relativas al nodo móvil pueden ser posibles también, utilizando otros mecanismos para intercambiar datagramas entre estos nodos, pero aquellas ubicaciones no hacen parte esencial del trabajo, ya que lo que se pretende es mostrar el funcionamiento de IP Móvil interna y externamente y todo lo relacionado con el manejo de datagramas y mensajes de anuncio y registro, y no las posibles extensiones que se podrían presentar con esta arquitectura.

Figura 15. Operación de IP Móvil versión 4



http://acimut.upf.es/moliver/OIL99.pdf

- El datagrama hacia el nodo móvil llega a la red local mediante enrutamiento IP estándar.
- El datagrama es interceptado por el agente local y es enviado a través de un túnel hacia la dirección temporal.
- El datagrama es sacado del túnel y entregado al nodo móvil.

- Para datagramas enviados por el nodo móvil, el enrutamiento IP estándar entrega cada uno a su destino. En la figura se muestra que el agente externo podría llegar a ser el router por defecto del nodo móvil.

Si un nodo móvil está usando una dirección temporal IP Co-located como se describió antes, el nodo móvil debe ser colocado en el enlace identificado por el prefijo de red de esta dirección temporal. De otra manera, los datagramas destinados a la dirección temporal no serían entregables.

Por ejemplo, la figura 15 ilustra el enrutamiento de datagramas hacia y desde un nodo móvil que se encuentra fuera de su red local, una vez que el nodo móvil se ha registrado con su agente local. En la figura anterior, el nodo móvil está utilizando una dirección temporal de agente externo, no una dirección temporal Co-located.

2.8 FORMATO DEL MENSAJE Y EXTENSIBILIDAD DEL PROTOCOLO

IP Móvil define un grupo de nuevos mensajes de control, enviados con UDP usando el muy conocido puerto 434. Aquí se definen los siguientes dos tipos de mensajes:

1. Solicitud de registro.
2. Respuesta de registro.

Hasta la fecha los valores para el tipo de mensaje, para mensajes de control de IP Móvil han sido especificados en los recientes estudios por parte de la IETF. Además, para el descubrimiento del agente, IP Móvil hace uso de los mensajes existentes de aviso del router y de solicitud del router, definidos para descubrimiento de router ICMP.

IP Móvil define un mecanismo de extensión general para permitir que se lleve información opcional en los mensajes de control de IP Móvil o en mensajes ICMP de descubrimiento del router. Algunas extensiones han sido especificadas para ser codificadas en formato simple de “valor de tipo de longitud”, las cuales son descritas más adelante en las secciones 2.8, 2.9, 2.10 y 2.11 y en la sección 4.5 completamente.

Las extensiones permiten que cantidades variables de información sean llevadas dentro de cada datagrama. El fin de la lista de extensiones es indicado por la longitud total del datagrama IP.

En IP Móvil son usados dos grupos de numeración de espacios que se mantienen separados, a partir de los cuales se asignan los valores de tipo de extensión:

- El primer grupo consiste en aquellas extensiones que pueden aparecer solo en mensajes de control IP Móvil (Aquellas enviadas para y desde el puerto UDP número 434). Aquí se definen los siguientes tipos, para extensiones que aparecen en los mensajes de control en IP Móvil:

    - 32 Autenticación Local-Móvil
    - 33 Autenticación Externa-Móvil
    - 34 Autenticación Local-Externa

- El segundo grupo consiste en aquellas extensiones que pueden aparecer solo en mensajes ICMP de descubrimiento del router. Aquí se definen los siguientes tipos, para extensiones que aparecen en los mensajes ICMP de descubrimiento del router:

    - 0 Relleno de un bit (codificado sin campo longitud ni de datos)
    - 16 Aviso del Agente de Movilidad
    - 19 Longitudes prefijas

Cada extensión individual, es descrita en detalle en una sección separada más adelante. A la fecha los valores para estos números de tipo de extensión están especificados en los estudios más recientes. Debido a la separación (ortogonalidad) de estos grupos, es concebible que dos extensiones que estén definidas en una fecha después podrían tener valores idénticos de tipo, tanto tiempo como una de las extensiones pueda ser usada solamente en los mensajes de control de IP Móvil y la otra pueda ser usada solamente en los mensajes ICMP de descubrimiento del router.

El campo Tipo en la estructura de extensiones de IP Móvil, puede soportar más de 255 extensiones (pasables y no pasables) únicamente identificables. Cuando una extensión numerada en cualquiera de estos grupos, dentro del rango 0 a 127 es encontrada pero no reconocida, el mensaje que contiene esa extensión debe ser descartado silenciosamente. Cuando una extensión numerada es encontrada en el rango 128 a 255 la cual no es reconocida, la

extensión particular es ignorada, pero el resto de las extensiones y los datos del mensaje deben ser procesados todavía. El campo de longitud de la extensión es usado para saltar el campo de datos en búsqueda de la siguiente extensión.

A menos que se utilice estructura adicional para los tipos de extensión, los nuevos desarrollos o adiciones a IP Móvil pueden requerir muchas más nuevas extensiones, que el espacio disponible puede agotar para los tipos de extensión. Se proponen dos nuevas estructuras de extensiones para solucionar este problema. Ciertos tipos de extensiones pueden ser agregadas, utilizando subtipos para identificar la extensión precisa, por ejemplo como se ha hecho con las Extensiones de Claves de Autenticación Genéricas. En muchos casos, esto puede reducir la velocidad de asignación para nuevos valores del campo de Tipo.

Siempre y cuando nuevas estructuras de extensión causen un uso eficiente del espacio de tipo de extensión, es recomendable que las extensiones nuevas de IP Móvil sigan uno de los dos formatos de extensión cada vez que pueda haber la posibilidad de agrupar extensiones relacionadas.

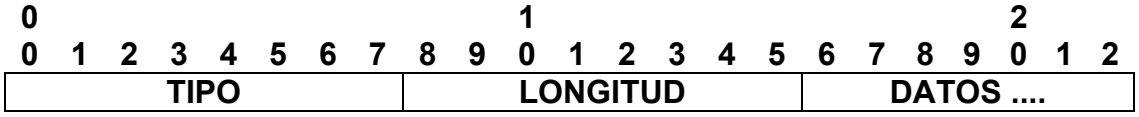
En las secciones posteriores se dan los detalles acerca de tres distintas estructuras para extensiones de IP Móvil:

- El formato de extensión simple
- El formato de extensión largo
- El formato de extensión corto

2.9 FORMATO DE EXTENSIÓN DEL VALOR DE TIPO- LONGITUD PARA EXTENSIONES IP MÓVILES

El formato del valor de tipo-longitud ilustrado en la figura 16 es utilizado para extensiones especificadas. Desde que esta estructura simple no fomente el uso más eficiente del espacio del tipo de extensión, es recomendado que las nuevas extensiones IP móviles sigan uno de los dos nuevos formatos especificados más adelante cuando pueda haber la posibilidad de agrupar las extensiones relacionadas.

Figura 16. Formato de extensión del valor de tipo-longitud para IPv4 Móvil



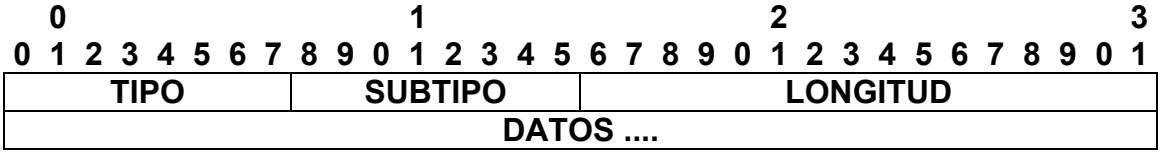
Autor.

- Tipo: indica el tipo particular de extensión.
- Longitud: indica la longitud (en bytes) del campo de datos dentro de esta extensión. La longitud NO incluye los bytes de Tipo ni de Longitud.
- Datos: los datos particulares asociados con esta extensión. Este campo puede ser cero o más bytes en longitud. El formato y la longitud del campo de Datos está determinado por el campo de Tipo y por el campo de Longitud.

2.10 FORMATO LARGO DE EXTENSIÓN

Este formato mostrado en la figura 17, es aplicable para extensiones no – saltables o pasables, las cuales cargan información de más de 256 bytes.

Figura 17. Formato largo de extensión



Autor.

El formato largo de extensión de la figura 17 requiere que los siguientes campos sean especificados como los primeros campos de la extensión.

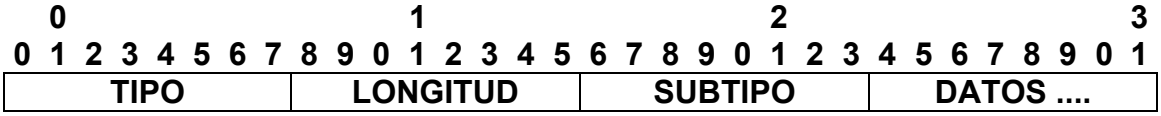
- Tipo: es el tipo, el cual describe un grupo de extensiones que tienen un tipo de datos común.
- Sub-tipo: es un único número dado para cada miembro en el tipo agregado.
- Longitud: indica la longitud (en bytes) del campo de datos dentro de esta extensión. NO incluye los bytes de Tipo, ni Longitud, ni Sub-tipo.
- Datos: son los datos asociados al subtipo de esta extensión. Esta especificación no necesita ninguna estructura adicional en los datos subtipo.

Desde que el campo de longitud sea 16 bits de amplio, la extensión de datos puede exceder los 256 bytes de longitud.

2.11 FORMATO CORTO DE EXTENSIÓN

Este formato de la figura 18, es compatible con las extensiones saltables definidas antes. No es aplicable para extensiones que requieren más de 256 bytes de datos. Para tales extensiones, se usa el formato descrito anteriormente en la figura 17.

Figura 18. Formato corto de extensión



Autor.

El formato corto de extensión requiere que los siguientes campos sean especificados como los primeros campos de la extensión:

- Tipo: es el tipo, el cual describe un grupo de extensiones que tienen un tipo de datos común.
- Sub-tipo: es un único número dado a cada miembro en el tipo agregado.
- Longitud: entero de 8 bits. Longitud de la extensión, en bytes, excluyendo el tipo de extensión y los campos de longitud de extensión. Este campo debe ser colocado en 1, más la longitud total del campo de datos.
- Datos: son los datos asociados con esta extensión. Esta especificación no necesita ninguna estructura adicional en los datos Subtipo.

3. DESCUBRIMIENTO DEL AGENTE

El descubrimiento del agente es el método por el cual un nodo móvil determina si está conectado actualmente a su red local o a una red externa, y mediante el cual un nodo móvil puede detectar cuando se ha movido de una red a otra. Aquí se especifican los métodos que también permiten al nodo móvil, mientras está conectado a una red externa, determinar la dirección temporal de agente externo, que está siendo ofrecida por cada agente externo sobre esa red.

IP Móvil extiende el descubrimiento de router ICMP como su primer mecanismo para Descubrimiento de agente. Un aviso de agente se forma mediante la inclusión de una extensión de aviso de movilidad del agente, en un mensaje de aviso del router ICMP. Un mensaje de solicitud de agente es idéntico a una solicitud de router ICMP, excepto que su TTL (Tiempo de Vida) IP debe ser colocado en 1. En las secciones subsiguientes se describen los formatos del mensaje y los procedimientos por los cuales los nodos móviles, agentes externos y agentes locales cooperan para realizar el descubrimiento del agente.

El aviso de agente y la solicitud del agente pueden no ser necesarios para capas de enlace que ya brindan esta funcionalidad. El método por el cual los nodos móviles establecen conexiones de capa de enlace con agentes posibles es un tema muy amplio y requiere un estudio adicional. Los procedimientos descritos más adelante, asumen que tal conectividad de capa de enlace ya ha sido establecida.

No se requiere autenticación para avisos de agente ni para mensajes de solicitud del agente. Ellos pueden ser autenticados utilizando el encabezado de autenticación IP, el cual no está relacionado con los mensajes descritos a lo largo del trabajo. La forma en la cual los mensajes de aviso y de solicitud pueden ser autenticados y su estudio de manera mucho más profunda también está fuera del objetivo del trabajo.

3.1 AVISO DEL AGENTE

Los avisos del agente son transmitidos por un agente de movilidad para advertir sus servicios sobre un enlace. Los nodos móviles usan estos avisos para determinar su punto actual de conexión o de acople a Internet. Un aviso

del agente es un aviso de router ICMP que ha sido extendido para llevar también una extensión de aviso del agente de movilidad y opcionalmente, una extensión de longitudes, una extensión de un bit de relleno u otras extensiones que pueden ser definidas en el futuro.

Dentro de un mensaje de aviso del agente, los campos de aviso de router ICMP del mensaje son requeridos para conformar las siguientes especificaciones adicionales:

- CAMPOS DE CAPA DE ENLACE
  - Dirección de destino: la dirección de destino de la capa de enlace de un aviso de agente unicast debe ser la misma que la dirección fuente de la capa de enlace de la solicitud del agente que provocó el aviso.

- CAMPOS IP
  - TTL: el TTL para todos los avisos de agente debe ser colocado en 1.
  - Dirección de destino: como se especificó para el descubrimiento del router ICMP, la dirección IP de destino de un aviso de agente multicast debe ser “todos los sistemas en este enlace” dirección (224.0.0.1) o “broadcast limitado” dirección (255.255.255.255). La dirección de broadcast de subnet-directa de la forma <prefijo>. <-1> no puede ser usada desde que los nodos móviles no conozcan generalmente el prefijo de la red externa. Cuando el aviso del agente es unicast para un nodo móvil, la dirección IP local del nodo móvil debería ser usada como la dirección de destino.

- CAMPOS ICMP
  - Código: el campo de código del aviso del agente es interpretado como sigue: 0 – El agente de movilidad maneja tráfico común, esto es, que actúa como un router para datagramas IP no necesariamente relacionados a nodos móviles. 16 – El agente de movilidad no enruta tráfico común. Sin embargo, todos los agentes externos deben (mínimamente) enviar a un router por defecto cualquier datagrama recibido de un nodo móvil registrado.
  - Tiempo de vida: la máxima longitud de tiempo que el aviso es considerado valido en ausencia de avisos más completos.
  - Dirección(es) de Router: ver secciones siguientes para una discusión de las direcciones que pueden aparecer en esta porción del aviso del agente.
  - Número de direcciones: el número de direcciones avisadas de router en este mensaje. Note que en un mensaje de aviso de agente, el número de direcciones de router especificadas en la porción de aviso de router ICMP del mensaje, puede ser colocado en 0.

Si el envío es periódicamente, el intervalo nominal al cual los avisos de agente son enviados, deberían no ser más largos que 1/3 del tiempo de vida dado del aviso en la cabecera ICMP. Este intervalo puede ser más corto que 1/3 del tiempo de vida avisado. Esto permite al nodo móvil perder tres avisos sucesivos antes de borrar el agente de la lista de agentes válidos. El tiempo actual de transmisión para cada aviso debe ser ligeramente aleatorio con el objeto de evitar sincronizaciones y colisiones subsecuentes con otro agente.

Los avisos pueden ser enviados por otros agentes (o con otros avisos de router enviados por otros routers). Note que este campo no tiene relación con el campo de "Registro de tiempo de vida" dentro de la extensión del agente de movilidad definida a continuación.

3.1.1 Extensión del Aviso del Agente de Movilidad. La extensión del aviso del agente de movilidad, sigue los campos de aviso de router ICMP, tal como se muestra en la figura 19. Es costumbre indicar que un mensaje de aviso de router ICMP, es también un aviso de agente que está siendo enviado por un agente de movilidad. La extensión del aviso del agente de movilidad se define en la figura 19:

Figura 19. Extensión del aviso del agente de movilidad

0								1								2								3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
TIPO								LONGITUD								NÚMERO DE SECUENCIA															
TIEMPO DE VIDA DE REGISTRO																R	B	H	F	M	G	r	T	RESERVADO						
CERO O MÁS DIRECCIONES TEMPORALES ...																															

Autor.

- Tipo: 16
- Longitud: (6 + 4*N), donde 6 cuenta para el número de bytes en el número de secuencia, registro de tiempo de vida, banderas y campos reservados, y N es el número de direcciones temporales anunciadas.
- Número de secuencia: la cuenta de los mensajes de aviso de agente enviados desde que el agente se ha inicializado.
- Tiempo de vida Registro: el tiempo de vida más largo (medido en segundos) que este agente está dispuesto a aceptar en cualquier solicitud de registro. Un valor de 0xffff indica infinito. Este campo no tiene relación al campo "tiempo de vida" dentro de la porción del aviso de router ICMP, del aviso del agente.
- R: registro requerido. El registro con este agente externo (u otro agente externo en este enlace) es requerido incluso cuando se está utilizando una dirección Co-located.
- B: ocupado. El agente externo no aceptará registros de nodos móviles adicionales.

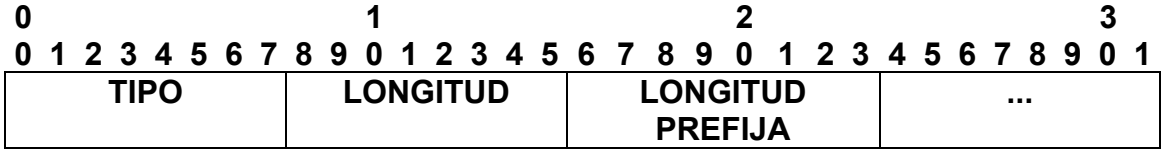
- H: agente local. Este agente ofrece servicio como un agente local sobre el enlace en el cual este mensaje de aviso del agente es enviado.
- F: agente externo. Este agente ofrece servicio como un agente externo sobre el enlace en cual este mensaje de aviso del agente es enviado.
- M: encapsulación mínima: este agente implementa la recepción de datagramas enviados a través de túneles que usan mínimo encapsulamiento.
- G: encapsulación GRE: este agente implementa la recepción de datagramas enviados a través de túneles que usan mínimo encapsulamiento.
- R: enviado como cero. Ignorado en recepción. NO debería estar asignado para ningún otro uso.
- T: el agente externo soporta túneles en reversa.
- Reservado: enviado como cero. Ignorado en recepción.
- Direcciones temporales: la(s) dirección(es) temporal(es) avisada(s) del agente externo brindada(s) por este agente externo. Un aviso del agente debe incluir al menos una dirección temporal, si el bit “F” está habilitado. El número de direcciones temporales presentes es determinado por el campo de longitud en la extensión.

Un agente local siempre debe estar preparado para servir al nodo móvil, para el cual él es el agente local. Un agente externo puede a veces estar muy ocupado para servir a nodos móviles adicionales; aún así, debe continuar enviando avisos de agente, así que cualquier nodo móvil ya registrado con él, sabrá que ellos no se han movido fuera del rango del agente externo y que el agente externo no ha fallado. Un agente externo puede indicar que está “muy ocupado” para permitir que nuevos nodos móviles se registren con él, enviando el bit “B” en sus avisos de agente. Un mensaje de aviso del agente NO debe tener el bit “B” habilitado, si el bit “F” no está tampoco habilitado. Además, al menos uno de los bits “F” y “H” debe habilitarse en cualquier mensaje enviado de aviso del agente.

Cuando un agente externo desea requerir el registro incluso de aquellos nodos móviles, lo cuales han adquirido una dirección temporal, él coloca el bit “R” en uno (1). Debido a que este bit aplica solamente para agentes externos, un agente NO debe colocar el bit “R” en uno (1), a menos que el bit “F” esté en uno (1) también.

3.1.2 Extensión de Longitudes Prefijas. La extensión de longitudes prefijas puede seguir la extensión del aviso de agente de movilidad. Es usada para indicar el número de bits del prefijo de red que aplica a cada dirección de router, listada en la porción de aviso de router ICMP, del aviso del agente. Note que las longitudes prefijas dadas NO aplican a la(s) dirección(es) temporal(es) listada(s) en la extensión de aviso del agente de movilidad. La extensión de longitudes prefijas se define como se muestra en la figura 20:

Figura 20. Formato de extensión de longitudes prefijas



Autor.

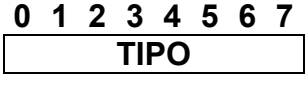
- Tipo: 19 (extensión de longitudes prefijas)
- Longitud: N, donde N es el valor (posiblemente cero) del campo número de dirección, en la porción de aviso de router ICMP, del aviso del agente.
- Longitud (es) prefija(s): el número de bits de guía que definen el número de red de la dirección de router correspondiente, listada en la porción de aviso del router ICMP del mensaje. La longitud prefija para cada dirección de router es codificada como un byte separado, de tal forma que las direcciones de router son listadas en la porción de aviso del router ICMP del mensaje.

En la sección número 11 del documento se describe la manera como puede ser utilizada la extensión de longitudes prefijas por un nodo móvil, cuando se determina si éste se ha movido..

3.1.3 Extensión de Relleno de Un Byte. Algunas implementaciones del protocolo IP insisten en rellenar los mensajes ICMP a un número par de bytes. Si la longitud ICMP de un aviso del agente es impar, esta extensión puede incluirse con el objetivo de hacer par la longitud ICMP. Note que esta extensión NO está destinada a ser una extensión de propósito general, para ser incluida con el objetivo de alinear palabras o el largo de diferentes campos del aviso del agente. Un aviso de agente NO debería incluir más de una extensión de relleno de un byte, y si se presenta, esta extensión debería ser la última extensión en el aviso del agente.

Debe observarse que a diferencia de otras extensiones usadas en IP Móvil, la extensión de relleno de un byte es codificada como un byte individual, sin campos de “longitud” y “datos” presentes. La extensión de relleno de un byte se define a continuación en la figura 21:

Figura 21. Extensión de relleno de un byte



Autor.

- Tipo 0 (extensión de relleno de un byte)

3.2 SOLICITUD DEL AGENTE

Una solicitud de agente es idéntica a una solicitud de router ICMP, con la restricción adicional de que el campo TTL de IP debe ser colocado en uno (1).

3.3 CONSIDERACIONES DEL AGENTE EXTERNO Y DEL AGENTE LOCAL

Cualquier agente de movilidad el cual no puede ser descubierto por un protocolo de capa de enlace, debe enviar avisos de agente. Un agente que puede ser descubierto por un protocolo de capa de enlace, debería también implementar avisos de agente. Sin embargo, los avisos no necesitan ser enviados, excepto cuando las políticas del sitio requieren registro con el agente (cuando el bit "R" está habilitado), o como una respuesta a una solicitud específica de agente. Todos los agentes de movilidad deben procesar paquetes que ellos reciben direccionados hacia el grupo multicast de agentes móviles, en la dirección 224.0.0.11. Un nodo móvil puede enviar una solicitud de agente a 224.0.0.11. Todos los agentes de movilidad deberían responder a las solicitudes de agente.

Los mismos procedimientos, defectos y constantes son usados en los mensajes de aviso del agente y en los mensajes de solicitud del agente, como se especificó para el descubrimiento del router ICMP, excepto que:

- Un agente de movilidad debe limitar la velocidad a la cual él envía avisos de agente broadcast o multicast; la máxima rata debería ser escogida de tal forma que los avisos no consuman una cantidad significativa de ancho de banda de la red,
- Un agente de movilidad que recibe una solicitud de router, NO debe requerir que la dirección IP de origen sea la dirección de un vecino (por ejemplo, una dirección que se ajusta a una de las direcciones propias del router sobre la interfase de llegada, bajo la máscara de subnet asociada con esa dirección del router)
- Un agente de movilidad puede ser configurado para enviar solamente avisos de agente en respuesta a un mensaje de solicitud de agente.

Si la red local no es una red virtual, entonces el agente local para cualquier nodo móvil debería ser ubicado sobre el enlace identificado por la dirección

local del nodo móvil, y los mensajes de aviso de agente enviados por el agente local en este enlace, deben tener el bit “H” habilitado. En este sentido, los nodos móviles sobre su propia red local serán capaces de determinar que ellos están verdaderamente en casa. Cualquier mensaje de aviso de agente enviado por el agente local sobre otro enlace al cual él puede ser acoplado (si él es un agente de movilidad sirviendo a más de un enlace), NO debe tener el bit “H” habilitado a menos que el agente local también sirva como un agente local (para otros nodos móviles) sobre ese enlace. Un agente de movilidad puede usar diferentes configuraciones para cada uno de los bits “R”, “H” y “F” sobre diferentes interfases de red.

Si la red local es una red virtual, la red local no tiene realización física externa hacia el agente local en sí. En este caso, no hay enlace de red física sobre el cual se envíen mensajes de aviso del agente advirtiendo el agente local. Los nodos móviles para los cuales ésta es la red local, siempre son tratados como si estuvieran lejos de su casa.

Sobre una subnet particular, todos los agentes de movilidad deben incluir la extensión de longitudes prefijas o todos ellos NO deben incluir esta extensión. De manera equivalente, está prohibido para algunos agentes sobre una red dada, que incluyan la extensión, pero para otros está prohibido que no la incluyan. De otro modo, uno de los algoritmos de detección de movimiento diseñados para nodos móviles no funcionará de manera apropiada. Esto es descrito en secciones posteriores.

3.3.1 Direcciones de Router Avisadas. La porción del aviso del router ICMP del aviso de agente puede contener una o más direcciones de router. Un agente debería solamente poner sus propias direcciones, si tiene alguna, en el aviso. Si aparece o no su propia dirección en las direcciones del router, un agente externo debe enrutar los datagramas que reciba de los nodos móviles registrados, tal como se describe más adelante.

3.3.2 Números de Secuencia y Manejo de Renovaciones. El número de secuencia en los rangos de 0 a 0xffff de los avisos de agente. Después de arrancar, un agente debe usar el número 0 para su primer aviso. Cada aviso subsiguiente, debe usar el número de secuencia más grande, con la excepción de que el número de secuencia 0xffff debe ser seguido por el número de secuencia 256. En este sentido, los nodos móviles pueden distinguir una reducción en el número de secuencia que ocurra, luego de un re-arranque a partir de una reducción, que resulte en la renovación del número de secuencia, después de que se consiga el valor 0xffff.

3.4 CONSIDERACIONES DEL NODO MÓVIL

Todo nodo móvil debe implementar solicitud de agente. Las solicitudes deberían solamente ser enviadas en ausencia de avisos de agente y cuando una dirección temporal no ha sido determinada a través de un protocolo de capa de enlace por otros medios. El nodo móvil utiliza los mismos procedimientos, falencias y constantes para solicitud de agente, como se especificó para los mensajes de solicitud de router ICMP, excepto que el nodo móvil puede solicitar más de una vez cada tres (3) segundos, y que el nodo móvil que no está conectado actualmente a un agente externo, puede solicitar más veces que el MÁXIMO DE SOLICITUDES.

La velocidad a la cual un nodo móvil envía solicitudes debe ser limitada por el nodo móvil. El nodo móvil puede enviar tres solicitudes iniciales a una velocidad máxima de una por segundo mientras busca un agente. Luego de esto, la velocidad a la cual las solicitudes son enviadas debe ser reducida de manera tal, que limite la sobrecarga en el enlace local. Las solicitudes subsiguientes deben ser enviadas utilizando un mecanismo de Backoff binario exponencial, doblando el intervalo entre solicitudes consecutivas, hasta un intervalo máximo. El intervalo máximo debería ser escogido apropiadamente, basado en las características del medio sobre el cual el nodo móvil está solicitando. El intervalo máximo debería ser al menos un minuto entre solicitudes.

Mientras se busca aún un agente, el nodo móvil NO debe incrementar la velocidad a la cual él envía solicitudes, a no ser que haya recibido una indicación positiva de que se ha movido a un nuevo enlace. Después del registro exitoso con un agente, el nodo móvil debería también aumentar la velocidad a la cual él enviará solicitudes, cuando él comienza a buscar un nuevo agente con el cual registrarse. La velocidad de solicitud incrementada puede volver a la velocidad máxima, pero entonces debe ser limitada de la manera descrita anteriormente. En todos los casos, los intervalos de solicitud recomendados son valores nominales. Los nodos móviles deben obtener de manera aleatoria sus tiempos de solicitud alrededor de estos valores nominales, como se especifica para el descubrimiento del router ICMP.

Los nodos móviles deben procesar los avisos de agente recibidos. Un nodo móvil puede distinguir un mensaje de aviso de agente, de otros usos del mensaje de aviso de router ICMP, examinando el número de direcciones advertidas y el campo IP de longitud total. Cuando el campo IP de longitud total, indica que el mensaje ICMP es más largo de lo necesario para el número de direcciones avisadas, los datos restantes son interpretados como una o más extensiones. La presencia de una extensión de aviso del agente de movilidad, identifica el aviso como un aviso de agente.

Si hay más de una dirección avisada, el nodo móvil debería tomar la primera dirección para su intento inicial de registro. Si el intento de registro falla, con un código de estado indicando rechazo por parte del agente externo, el nodo móvil puede volver a intentar con cada dirección avisada posterior que esté en turno.

Cuando están en uso múltiples métodos de descubrimiento de agente, el nodo móvil debería primero intentar el registro con agentes, incluyendo extensiones de aviso de agente de movilidad dentro sus avisos, en vez de aquellos descubiertos por otros medios. Esta preferencia maximiza la probabilidad de que el registro será reconocido, minimizando de este modo, el número de intentos de registro.

Un nodo móvil debe ignorar los bits reservados en los avisos de agente, en contra de descartar tales avisos. En este sentido, nuevos bits pueden ser definidos después, sin afectar la habilidad de los nodos móviles de usar avisos, incluso cuando bits recién definidos no son entendidos.

3.4.1 Registro Requerido. Cuando el nodo móvil recibe un aviso de agente con el bit “R” habilitado, el nodo móvil debería registrarse a través del agente externo, incluso cuando el nodo móvil debe ser capaz de adquirir su propia dirección temporal Co-located. Esta característica pretende permitir a los sitios hacer cumplir las políticas de visitas (tales como contabilidad) las cuales requieren intercambios de autorizaciones.

Si los bits reservados antes, requieren alguna clase de monitoreo / obligación en el enlace externo, los agentes externos implementando la nueva especificación para los bits reservados antes, pueden habilitar el bit “R”. Esto tiene el efecto de obligar al nodo móvil a registrarse a través del agente externo, así el agente externo podría entonces monitorear / hacer cumplir las políticas.

3.4.2 Detección de Movimiento. Dos mecanismos primarios están dados para que los nodos móviles detecten cuando ellos se hayan movido de una subred a otra. Otros mecanismos pueden ser utilizados también. Cuando un nodo móvil detecta que se ha movido, debería registrarse con una dirección temporal apropiada en la nueva red externa. Sin embargo, el nodo móvil NO debe registrarse más frecuentemente que una vez por segundo en promedio. Esto es especificado en secciones siguientes.

- Algoritmo 1: el primer método de detección de movimiento está basado en el campo de tiempo de vida, dentro del cuerpo principal del la porción ICMP del aviso de router, del aviso del agente. Un nodo móvil debería grabar el tiempo de vida recibido en cualquier aviso de agente, hasta que ese tiempo de vida expire. Si el nodo móvil falla en recibir otro aviso del mismo agente dentro del tiempo de vida especificado, él debería asumir que ha perdido contacto con ese agente. Si el nodo móvil previamente ha recibido un aviso de agente de otro agente, para el cual el campo de tiempo de vida no ha expirado aún, el nodo móvil puede inmediatamente intentar registrarse con ese otro agente. De otra manera, el nodo móvil debería intentar descubrir un nuevo agente con el cual se registre.

- Algoritmo 2: el segundo método utiliza prefijos de red. La extensión de longitudes prefijas puede ser usada en algunos casos por un nodo móvil, para determinar si un aviso de agente recientemente recibido, fue recibido sobre la misma subnet, como la dirección temporal actual del nodo móvil. Si los prefijos difieren, el nodo móvil puede asumir que se ha movido. Si un nodo móvil está utilizando actualmente una dirección temporal de agente externo, el nodo móvil NO debería usar este método de detección de movimiento, a menos que tanto el agente actual como el nuevo agente incluyan la extensión de longitudes prefijas en sus respectivos avisos de agente; si esta extensión está perdida en alguno de los dos avisos, este método de detección NO debería ser utilizado. De manera similar, si un nodo móvil está usando una dirección temporal Co-located, él no debería usar este método de detección de movimiento, a menos que el nuevo agente incluya la extensión de longitudes prefijas en su aviso y que el nodo móvil conozca el prefijo de red de su actual dirección temporal Co-located. Al expirar su registro actual, si este método indica que el nodo móvil se ha movido, en vez de volverlo a registrar con su actual dirección temporal, un nodo móvil puede escoger registrarse preferiblemente con un agente externo, enviando el nuevo aviso con el prefijo de red diferente. El aviso de agente sobre el cual se basa el nuevo registro, NO debe haber expirado de acuerdo con su campo de tiempo de vida.

3.4.3 Regreso a Casa. Un nodo móvil puede detectar que ha regresado a su red local cuando recibe un aviso de agente de su propio agente local. Si es así, él debería desregistrarse con su agente local. Antes de intentar desregistrarse, el nodo móvil debería configurar su tabla de enrutamiento apropiadamente para su red local. Además, si la red local está usando ARP, el nodo móvil debe seguir los procedimientos descritos en la sección 5.6 respecto a ARP, ARP Proxy y ARP gratuito.

3.4.4 Números de Secuencia y Manejo de Renovación. Si un nodo móvil detecta dos valores sucesivos de número de secuencia, en los avisos de agente provenientes del agente externo con el cual él está registrado, el

segundo de ellos es menor que el primero y está dentro del rango de 0 a 255, el nodo móvil debería registrarse de nuevo. Si el segundo valor es menor que el primero pero mayor o igual a 256, el nodo móvil debería asumir que el número de secuencia ha sobrepasado su máximo valor (0xffff), y que su nuevo re-registro no es necesario.

4. REGISTRO

El registro IP Móvil provee un mecanismo flexible para que los nodos móviles comuniquen su actual información alcanzable al agente local. Este es el método por el cual los nodos móviles:

- Solicitan servicios por anticipado cuando se visita una red externa,
- Informan a su agente local acerca de su dirección temporal actual,
- Renuevan un registro el cual está próximo a expirar, y/o
- Se desregistra cuando ellos regresan a su casa.

Los mensajes de registro intercambian información entre un nodo móvil, (opcionalmente) un agente externo y un agente local. El registro crea o modifica un vínculo de movilidad en su agente local, asociando la dirección local del nodo móvil, con su dirección temporal para el tiempo de vida especificado.

Varias diferentes capacidades (opcionales) están disponibles por medio del procedimiento de registro, el cual habilita un nodo móvil para:

- Descubrir su dirección local, si el nodo móvil no está configurado con esta información.
- Mantener registros simultáneos múltiples, de manera tal, que una copia de cada datagrama será enviado a través de un túnel, a cada dirección temporal activa.
- Desregistrar direcciones temporales específicas, mientras se mantienen otros vínculos de movilidad, y
- Descubrir la dirección de un agente local si el nodo móvil no está configurado con esta información.

4.1 VISIÓN GENERAL DEL REGISTRO

IP Móvil define dos diferentes procedimientos de registro, uno por medio de un agente externo que releva el registro al agente local del nodo móvil, y otro directamente con el agente local del nodo móvil. Las siguientes reglas determinan cual de estos dos procedimientos de registro se usan en cualquier circunstancia particular:

- Si un nodo móvil está registrando una dirección temporal de agente externo, el nodo móvil debe registrarse por medio de ese agente externo.
- Si un nodo móvil está usando una dirección temporal Co-located, y recibe un aviso de agente de un agente externo sobre el enlace en el cual está usando esta dirección temporal, el nodo móvil debería registrarse por medio de ese agente externo (o por medio de otro agente externo sobre este enlace) si el bit "R" está habilitado en el mensaje de aviso de agente recibido.
- Si por el contrario el nodo móvil está usando una dirección temporal Co-located, el nodo móvil debe registrarse directamente con su agente local.
- Si un nodo móvil ha regresado a su red local y está (des)registrándose con su agente local, el nodo móvil debe registrarse directamente con su agente local.

Ambos procedimientos de registro envuelven el intercambio de mensajes de solicitud de registro y de respuesta de registro. Cuando se registra por medio de un agente externo, el procedimiento de registro requiere los siguientes cuatro mensajes:

- El nodo móvil envía una solicitud de registro al agente externo posible para empezar el proceso de registro.
- El agente externo procesa la solicitud de registro y la releva al agente local.
- El agente local envía una respuesta de registro al agente externo para admitir o denegar la solicitud.
- El agente externo procesa la respuesta de registro y la releva al nodo móvil para informarle de la disposición de su solicitud.

Cuando el nodo móvil por el contrario se registra directamente con su agente local, el procedimiento de registro requiere solo los siguientes dos mensajes:

- El nodo móvil envía una solicitud de registro al agente local.
- El agente local envía una respuesta de registro al nodo móvil, admitiendo o denegando la solicitud.

Los mensajes de registro definidos en las secciones siguientes utilizan el Protocolo de Datagramas de Usuario (UDP User Datagram Protocol). Un checksum del UDP diferente de cero (0) debería ser incluido en el encabezado, y debe ser revisado por el receptor. Un checksum del UDP igual a cero (0) debería ser aceptado por el receptor. El comportamiento del nodo móvil y del agente local con respecto a su mutuo reconocimiento de paquetes con

checksum de UDP iguales a cero, debería se definido como parte de la asociación de seguridad de movilidad que existe entre ellos.

4.2 AUTENTICACIÓN

Cada nodo móvil, agente externo y agente local debe ser capaz de soportar una asociación de seguridad de movilidad para entidades móviles, listadas por sus direcciones SPI e IP. En el caso del nodo móvil, esta debe ser su dirección local. Para requerimientos de soporte de algoritmos de autenticación hay una parte especial en capítulos más adelante. Los mensajes de autenticación entre un nodo móvil y su agente local deben ser autenticados con una extensión de habilitación de autorización, por ejemplo, la extensión de autenticación móvil - local. Esta extensión debe ser la primera extensión de autenticación; otras extensiones de agente específico pueden ser agregadas al mensaje después de que el nodo móvil computa la autenticación.

4.3 SOLICITUD DE REGISTRO

Un nodo móvil se registra con su agente local usando mensaje de solicitud de registro como el de la figura 22, de tal forma que su agente local pueda crear o modificar un vínculo de movilidad para ese nodo móvil (por ejemplo, con un nuevo tiempo de vida). La solicitud puede ser relevada al agente local por el agente externo, a través del cual el nodo móvil está registrándose, o puede ser enviado directamente al agente local en el caso en el cual el nodo móvil está registrando una dirección temporal Co-located.

- CAMPOS IP
  - Dirección de origen: típicamente la dirección de interfase desde la cual el mensaje es enviado.
  - Dirección de destino: típicamente aquella del agente externo o del agente local.

En secciones posteriores hay más detalles.

- CAMPOS UDP
  - Puerto fuente: variable
  - Puerto de destino: 434

El encabezado UDP está seguido por los campos IP que se muestran a continuación:

Figura 22. Mensaje de solicitud de registro

0	1	2	3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1			
TIPO	S B D M G r T x	TIEMPO DE VIDA	
DIRECCIÓN LOCAL			
AGENTE LOCAL			
DIRECCIÓN TEMPORAL			
IDENTIFICACIÓN			
EXTENSIONES			

Autor.

- Tipo: 1 (solicitud de registro)
- S: vínculos Simultáneos. Si el bit “S” está habilitado, el nodo móvil está solicitando que el agente local retenga sus vínculos de movilidad anteriores, como se describe más adelante.
- B: datagramas Broadcast. Si el bit “B” está habilitado, el nodo móvil solicita que el agente local envíe por un túnel hacia él, cualquier datagrama broadcast que el agente reciba sobre la red local, como se describe más adelante.
- D: desencapsulamiento por el nodo móvil. Si el bit “D” está habilitado, el nodo móvil desencapsulará por si mismo los datagramas que son enviados hacia una dirección temporal. Esto es, el nodo móvil está usando una dirección temporal Co-located.
- M: encapsulamiento Mínimo. Si el bit “M” está habilitado, el nodo móvil solicita que su agente local use encapsulamiento mínimo para los datagramas enviados por túnel al nodo móvil.
- G: encapsulamiento GRE. Si el bit “G” está habilitado, el nodo móvil solicita que su agente local use encapsulamiento GRE para datagramas enviados por túnel al nodo móvil.
- r: enviado como cero. Ignorado en recepción. NO debería ser colocado para cualquier otro uso.
- T: solicitud de Túnel en reversa.
- x: enviado como cero. Ignorado en recepción.
- Tiempo de vida: el número de segundos restantes antes de que se considere que el registro ha expirado. Un valor de cero indica una solicitud para desregistro. Un valor de 0xffff indica infinito.
- Dirección local: la dirección IP del nodo móvil.
- Agente local: La dirección IP del agente local del nodo móvil.
- Dirección temporal: La dirección para el final del túnel.

- Identificación: un número de 64 bits, construido por el nodo móvil, usado para ajustar solicitudes de registro con respuestas de registro, y para proteger contra ataques repetitivos de mensajes de registro.
- Extensiones: la porción fija de la solicitud de registro está seguida por una o más de las extensiones las cuales son listadas en la sección de Extensiones de Registro. Una extensión de habilitación de autorización debe estar incluida en todas las solicitudes de registro. Para información sobre el orden relativo en el cual extensiones diferentes, cuando están presentes, deben ser colocadas en un mensaje de solicitud de registro, se pueden ver secciones posteriores, específicamente el numeral 4.5 y sus numerales subsiguientes 4.5.1, 4.5.2, 4.5.3 y 4.5.4.

4.4 RESPUESTA DE REGISTRO

Un agente de movilidad típicamente regresa un mensaje de respuesta de registro a un nodo móvil que ha enviado un mensaje de solicitud de registro. Si el nodo móvil está solicitando servicio de un agente externo, ese agente externo típicamente recibirá la respuesta del agente local y enseguida la relevará al nodo móvil. Los mensajes de respuesta contienen el código necesario para informar al nodo móvil acerca del estado de su solicitud, junto con el tiempo de vida admitido por el agente local, el cual puede ser más pequeño que la solicitud original, tal como se muestra en la figura 23.

El agente externo NO debe incrementar el tiempo de vida seleccionado por el nodo móvil en la solicitud de registro, ya que el tiempo de vida es cubierto por una extensión de autenticación, la cual habilita la autorización por el agente local. Tal extensión contiene datos de autenticación los cuales no pueden ser correctamente (re)computados por el agente externo. El agente local NO debe incrementar el tiempo de vida seleccionado por el nodo móvil en la solicitud de registro, ya que si se hace esto se podría incrementar por encima del máximo tiempo de vida de registro permitido por el agente externo. Si el tiempo de vida recibido en la respuesta de registro es mayor que aquel en la solicitud de registro, el tiempo de vida en la solicitud debe ser usado. Cuando el tiempo de vida recibido en la respuesta de registro es menor que aquel en la solicitud de registro, el tiempo de vida en la respuesta debe ser usado.

- CAMPOS IP
  - Dirección de origen: típicamente copiada de la dirección de destino de la solicitud de registro, a la cual el agente está respondiendo. Para mayores detalles se pueden consultar algunas secciones posteriores.
  - Dirección de destino: copiada de la dirección de origen de la solicitud de registro, a la cual el agente está respondiendo.

- CAMPOS UDP
  - Puerto de origen: variable.
  - Puerto de destino: copiado del puerto de origen de la correspondiente solicitud de registro.

La cabecera UDP está seguida por los campos IP Móvil mostrados a continuación:

Figura 23. Mensaje de respuesta de registro

0								1								2								3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
TIPO								**CÓDIGO**								**TIEMPO DE VIDA**															
DIRECCIÓN LOCAL																															
AGENTE LOCAL																															
DIRECCIÓN TEMPORAL																															
IDENTIFICACIÓN																															
EXTENSIONES																															

Autor.

- Tipo: 3 (respuesta de registro)
- Código: un valor indicando el resultado de la solicitud de registro. Ver más adelante para una lista de los valores de código definidos actualmente.
- Tiempo de vida: si el campo de código indica que el registro fue aceptado, el campo de tiempo de vida es colocado en el número de segundos restantes antes de que el registro se considere expirado. Un valor de cero indica que el nodo móvil ha sido desregistrado. Un valor de 0xffff indica infinito. Si el campo de código indica que el registro fue denegado, el contenido del campo de tiempo de vida no está especificado y debe ser ignorado en recepción.
- Dirección local: la dirección IP del nodo móvil.
- Agente local: la dirección IP del agente local del nodo móvil.
- Identificación: número de 64 bits usado para ajustar solicitudes de registro con respuestas de registro y para proteger contra ataques repetitivos de mensajes de registro. El valor está basado en el campo de identificación del mensaje de solicitud de registro del nodo móvil y en el estilo de protección de repetición usado en el contexto de seguridad, entre el nodo móvil y su agente local (definido por la asociación de seguridad de movilidad entre ellos y el valor SPI en la extensión de habilitación de autorización).
- Extensiones: la porción fija de la respuesta de registro está seguida por una o más de las extensiones listadas en la sección de Extensiones de Registro. Una extensión de habilitación de autorización debe estar incluida en todas

las respuestas de registro regresadas por el agente local. Para las reglas para colocar extensiones a los mensajes de respuesta se pueden consultar secciones posteriores.

Los valores siguientes están definidos para usar dentro del campo de código.

Registro exitoso:
0 – registro aceptado.
1 – registro aceptado, pero uniones de movilidad simultáneas no soportadas.

Registro denegado por el agente externo:
64 – razón no especificada
65 – prohibido administrativamente
66 – recursos insuficientes
67 – autenticación fallida del nodo móvil
69 – muy largo el tiempo de vida solicitado
70 – solicitud formada pobremente
71 – respuesta formada pobremente
72 – encapsulamiento solicitado no disponible
73 – reservado y no disponible
TBD-IANA – dirección de agente local inválida
77 – dirección temporal inválida
78 – tiempo fuera de registro
80 – red local inalcanzable (error ICMP recibido)
81 – host del agente local inalcanzable (error ICMP recibido)
82 – puerto del agente local inalcanzable (error ICMP recibido)
88 – agente local inalcanzable (otro error ICMP recibido)

Registro denegado por el agente local:
128 –razón no especificada
129 – prohibido administrativamente
130 – recursos insuficientes
131 – autenticación fallida del nodo móvil
132 – autenticación fallida del agente externo
133 – identificación de registro no ajustada
134 – solicitud formada pobremente
135 – muchas uniones de movilidad simultáneas
136 – dirección de agente local desconocida

A la fecha, los valores del campo de código están especificados en los estudios más recientes “Números asignados”.

4.5 EXTENSIONES DE REGISTRO

4.5.1 Computando Valores de Extensión de Autenticación. El valor computado que autentica para cada extensión de autenticación debe proteger los siguientes campos del mensaje de registro:

- La carga útil (esto es, los datos de solicitud de registro o de respuesta de registro)
- Todas las extensiones previas en su totalidad, y
- El tipo, longitud y SPI de esta extensión.

El algoritmo de autenticación por defecto usa HMAC-MD5 para computar un "resumen de mensaje" de 128 bits del mensaje de registro. Los datos sobre los cuales se computa HMAC se definen como:

- La carga útil (esto es, los datos de solicitud de registro o de respuesta de registro)
- Todas las extensiones previas en su totalidad, y
- El tipo, longitud y SPI de esta extensión.

Note que el campo que autentica por si mismo y la cabecera UDP NO están incluidos en el computo del valor por defecto que autentica.

Para información acerca de los requerimientos de soporte para códigos de autenticación de mensaje, los cuales están para ser utilizados con las variadas extensiones de autenticación, se pueden consultar algunas secciones posteriores.

El Índice de Parámetros de Seguridad (SPI en inglés) dentro de cualquier extensión de autenticación define el contexto de seguridad, que es usado para computar el valor autenticador, y el cual debe ser utilizado por el receptor para revisar dicho valor. En particular, el SPI selecciona el algoritmo y el modo de autenticación (sección 6.1) y el secreto (una clave compartida o un par de llaves pública y privada apropiado) usado en el cómputo del autenticador. Con el objetivo de asegurar la interoperabilidad entre diferentes implementaciones del protocolo IP Móvil, una implementación debe ser capaz de asociar cualquier valor SPI con cualquier algoritmo y modo de autenticación que este implemente. Además, todas las implementaciones de IP Móvil deben implementar el algoritmo de autenticación por defecto (HMAC-MD5) mencionado antes.

4.5.2 Extensión de Autenticación Móvil-Local. Al menos una extensión de habilitación de autorización debe estar presente en todas las solicitudes de registro y también en todas las respuestas de registro generadas por el agente local. La extensión de autenticación móvil-local mostrada en la figura 24, es siempre una habilitación de autorización para mensajes de registro especificados en el presente trabajo. Este requerimiento promete eliminar problemas que resultan a partir de propagación no controlada de re-direccionamientos remotos en Internet. El lugar de la extensión de habilitación de autorización marca el final de los datos a ser autenticados por el agente que autoriza, interpretando esa extensión de habilitación de autorización.

Figura 24. Extensión de autenticación móvil-local

0								1								2								3		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
TIPO								**LONGITUD**								**SPI ...**										
... SPI (Cont.)																**AUTENTICADOR ...**										

Autor.

- Tipo: 32
- Longitud: 4 más el número de bytes en el autenticador.
- SPI: Índice de Parámetros de Seguridad (4 bytes). Un identificador opaco.
- Autenticador: (longitud variable)

4.5.3 Extensión de Autenticación Móvil-Exterior. Esta extensión que se muestra en la figura 25, puede estar incluida en solicitudes y respuestas de registro, en casos en los cuales una asociación de seguridad de movilidad existe entre el nodo móvil y el agente externo. Para mayor información acerca de los requerimientos de soporte para códigos de autenticación de mensaje se pueden consultar secciones posteriores.

Figura 25. Extensión de autenticación móvil-exterior

0								1								2								3		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
TIPO								**LONGITUD**								**SPI ...**										
... SPI (Cont.)																**AUTENTICADOR ...**										

Autor.

- Tipo: 33
- Longitud: 4 más el número de bytes en el autenticador.
- SPI: Índice de Parámetros de Seguridad (4 bytes). Un identificador opaco
- Autenticador: (longitud variable)

4.5.4 Extensión de autenticación Externa-Local. Esta extensión que se observa en la figura 26, puede estar incluida en solicitudes y respuestas de registro, en casos en los cuales una asociación de seguridad de movilidad existe entre el agente externo y el agente local. Para mayor información acerca de los requerimientos de soporte para códigos de autenticación de mensaje favor remitirse a la sección posterior 6.1 del capítulo 6.

Figura 26. Extensión de autenticación externa-local

0								1								2								3		
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
TIPO								**LONGITUD**								**SPI ...**															
... SPI (Cont.)																**AUTENTICADOR ...**															

Autor.

- Tipo: 34
- Longitud: 4 más el número de bytes en el autenticador.
- SPI: Índice de Parámetros de Seguridad (4 bytes). Un identificador opaco
- Autenticador: (longitud variable)

Con el objetivo de ejecutar la autenticación, el agente local y el agente externo tienen que haber configurado una asociación de seguridad, que sea capaz de ser catalogada por el uso del SPI y la dirección temporal asociada con el agente externo. Esta dirección temporal debe ser usada como la dirección IP de origen de la solicitud de registro, que contiene la extensión de autenticación externa-local. Cuando la extensión es utilizada con un mensaje de respuesta de registro, la dirección del agente externo debe usarse como la dirección IP de destino en el encabezado IP.

4.6 CONSIDERACIONES DEL NODO MOVIL

Un nodo móvil debe estar configurado con una máscara de red y una asociación de seguridad de movilidad para cada uno de sus agentes locales. Además, un nodo móvil puede estar configurado con su dirección local y la dirección IP de uno o más de sus agentes locales; de otro modo, el nodo móvil puede descubrir un agente local, usando los procedimientos descritos más adelante.

Si el nodo móvil no está configurado con una dirección local, él puede usar la extensión NAI del Nodo Móvil para identificarse a si mismo y colocar el campo

de dirección local de la solicitud de registro en 0.0.0.0. En este caso, el nodo móvil debe ser capaz de asignar su dirección local, después de extraer esta información de la respuesta de registro del agente local.

Para cada registro que se está llevando a cabo, el nodo móvil mantiene la siguiente información:

- La dirección de capa de enlace del agente externo, al cual se le envió la solicitud de registro, si es aplicable.
- La dirección IP de destino de la solicitud de registro.
- La dirección temporal usada en el registro.
- El valor de identificación enviado en el registro.
- El tiempo de vida solicitado originalmente, y
- El tiempo de vida restante del registro que se está llevando a cabo.

Un nodo móvil debería iniciar un registro en cualquier momento que él detecte un cambio en su conectividad de red. Para los métodos por los cuales los nodos móviles pueden hacer tal determinación se pueden consultar secciones anteriores. Cuando está lejos de casa, la solicitud de registro del nodo móvil permite a su agente local crear o modificar una ligadura de movilidad para él. Cuando está en casa, la solicitud de (des) registro del nodo móvil, permite a su agente local borrar cualquier ligadura de movilidad previa para él. Un nodo móvil opera sin el soporte de funciones de movilidad cuando está en casa.

Hay otras condiciones bajo las cuales el nodo móvil debería (re) registrarse con su agente externo, tales como, cuando el nodo móvil detecta que el agente externo se ha re-arrancado como se especificó más atrás y cuando el tiempo de vida de registro actual está cerca de expirar.

En la ausencia de indicaciones de la capa de enlace acerca de cambios en el punto de acople, los avisos de agente de nuevos agentes NO deberían causar que un nodo móvil intente un nuevo registro, si su registro actual no ha expirado y todavía está recibiendo avisos de agente del agente externo con el cual está actualmente registrado. En ausencia de indicaciones de la capa de enlace, un nodo móvil NO debe intentar registrarse más de una vez por segundo.

Un nodo móvil puede registrarse con un agente diferente cuando los protocolos de la capa de transporte indican retransmisiones excesivas. Un nodo móvil NO puede considerar la recepción de un ICMP redireccionado desde un agente externo que está actualmente brindándole servicio, como razón para registrarse

con un nuevo agente externo. Dentro de estas consideraciones, el nodo móvil puede registrarse de nuevo en cualquier momento.
En capítulos posteriores se muestran algunos ejemplos de cómo deberían ser configurados los campos en los mensajes de registro, en algunos escenarios de registro típicos.

4.6.1 Enviando Solicitudes de Registro. Las secciones siguientes especifican detalles para los valores que el nodo móvil debe suministrar, en los campos de los mensajes de solicitud de registro.

❖ Campos IP

Esta sección provee las reglas específicas por las cuales los nodos móviles toman valores para los campos del encabezado IP de una solicitud de registro.

- Dirección IP de origen
  - Cuando se está registrando en una red externa con una dirección temporal Co-located, la dirección IP de origen debe ser la dirección temporal.
  - De otro modo, si el nodo móvil no tiene una dirección local, la dirección IP de origen debe ser 0.0.0.0.
  - En las demás circunstancias, la dirección IP de origen debe ser la dirección local del nodo móvil.

- Dirección IP de destino
  - Cuando un nodo móvil ha descubierto al agente con el cual se está registrando, por medio de algunos medios (por ejemplo capa de enlace) que no provee la dirección IP del agente (la dirección IP del agente es desconocida para el nodo móvil), entonces se debe usar la dirección multicast de la “totalidad de los agentes de movilidad” (224.0.0.11). En este caso, el nodo móvil debe usar la dirección unicast de capa de enlace del agente, con el objetivo de entregar el datagrama al agente correcto.
  - Cuando se está registrando con un agente externo, la dirección del agente externo que se aprendió a partir de la dirección IP de origen del aviso de agente correspondiente, debe ser utilizada. Esta puede ser una dirección la cual no aparece como una dirección temporal avisada en el aviso de agente. Además, cuando se está transmitiendo este mensaje de solicitud de registro, el nodo móvil debe usar una dirección de destino de capa de enlace, copiada de la dirección de origen de la capa de enlace del mensaje de aviso de agente, en el cual aprendió esta dirección IP del agente externo.
  - Cuando el nodo móvil está registrándose directamente son su agente local y conoce la dirección IP (unicast) de su agente local, la dirección de destino debe colocarse en esta dirección.

- Si el nodo móvil se está registrando directamente con su agente local, pero no conoce la dirección IP de su agente local, el nodo móvil puede usar resolución dinámica de dirección de agente local, para determinar automáticamente la dirección IP de su agente local. En este caso, la dirección IP de destino se configura con la dirección broadcast de subred directa de la red local del nodo móvil. Esta dirección NO debe ser usada como la dirección IP de destino si el nodo móvil se está registrando por medio de un agente externo, aunque puede ser usada como la dirección de agente local en el cuerpo de la solicitud de registro, cuando se está registrando por medio de un agente externo.

- Tiempo de vida IP: el campo TTL (Time To Live) IP debe estar puesto en 1, si la dirección IP de destino está colocada en la dirección multicast de la "totalidad de los agentes de movilidad", como se describió antes. De lo contrario un valor apropiado debería ser escogido de acuerdo con el estándar IP de costumbre.

❖ Campos de Solicitud de Registro

Esta sección provee las reglas por las cuales, los nodos móviles toman valores para los campos dentro de la porción fija de una solicitud de registro.

Un nodo móvil puede habilitar el bit "S" con el objetivo de solicitar que el agente local mantenga enlace(s) de movilidad previo(s). De lo contrario, el agente local borra cualquier atadura y las remplaza con nuevas ataduras especificadas en la solicitud de registro. Es probable que múltiples ataduras de movilidad simultáneas sean útiles, cuando un nodo móvil usando al menos una interfase de red inalámbrica, se mueve dentro de un rango de transmisión inalámbrico, de más de un agente externo. Explícitamente, IP permite la duplicación de datagramas. Cuando el agente local permite ataduras simultáneas, él enviará por medio de un túnel una copia separada de cada datagrama que llega a cada dirección temporal, y el nodo móvil recibirá múltiples copias de los datagramas destinados a él.

El nodo móvil debería habilitar el bit "D" si está registrándose con una dirección temporal Co-located. De lo contrario, el bit "D" NO debe ser habilitado.

Un nodo móvil puede habilitar el bit "B", para solicitarle a su agente local que haga seguir hacia él una copia de datagramas broadcast recibidos por su agente local de la red local. El método usado por el agente local para hacer pasar los datagramas broadcast depende del tipo de dirección temporal registrado por el nodo móvil, como se determina por el bit "D" en la solicitud de registro del nodo móvil:

- Si el bit “D” está habilitado, entonces el nodo móvil ha indicado que desencapsulará cualquier datagrama enviado por túnel a esta dirección temporal como tal (el nodo móvil esta utilizando una dirección temporal Co-located). En este caso, para hacer seguir un datagrama broadcast recibido, hacia el nodo móvil, el agente local debe enviarlo por túnel a esta dirección temporal. El nodo móvil “saca del túnel” el datagrama recibido de la misma forma como lo hace con cualquier datagrama enviado por túnel directamente hacia él.
- Si el bit “D” NO está habilitado entonces el nodo móvil ha indicado que está usando una dirección temporal de agente externo, y que el agente externo desencapsulará así, los datagramas que lleguen, antes de hacerlos seguir al nodo móvil. En este caso, para hacer seguir un datagrama broadcast recibido, hacia el nodo móvil, el agente local debe primero encapsular el datagrama broadcast en un datagrama unicast dirigido a la dirección local del nodo móvil, y entonces enviar por un túnel el datagrama resultante, hacia la dirección temporal del nodo móvil.

Cuando se desencapsula por un agente externo, el datagrama interno será pues un datagrama IP unicast dirigido hacia el nodo móvil, identificando al agente externo el destino propuesto del datagrama broadcast encapsulado, y será entregado al nodo móvil de la misma forma que cualquier datagrama entrante, enviado por túnel para el nodo móvil. El agente externo NO debe desencapsular el datagrama broadcast encapsulado y NO debe usar una red local broadcast para transmitirlo hacia el nodo móvil. El nodo móvil debe desencapsular así, el datagrama broadcast encapsulado por si mismo, de tal forma que NO debe habilitar el bit “B” en su solicitud de registro en este caso, a menos que sea capaz de desencapsular datagramas.

El nodo móvil puede solicitar formas alternativas de encapsulamiento habilitando el bit “M” y / o el bit “G”, pero solamente si el nodo móvil está desencapsulando sus propios datagramas (el nodo móvil está utilizando una dirección temporal Co-located) o si su agente externo le ha indicado claramente soporte para estas formas de encapsulamiento colocando los bits correspondientes en la extensión del aviso de agente de movilidad de un aviso de agente recibido por el nodo móvil. De lo contrario, el nodo móvil NO debe colocar estos bits.

El campo de tiempo de vida se escoge como sigue:

- Si el nodo móvil está registrándose con un agente externo, el tiempo de vida NO debería exceder el valor en el campo de tiempo de vida de registro, del mensaje de aviso del agente, recibido desde el agente externo. Cuando el método por el cual se aprende la dirección temporal no incluye un tiempo de

vida, se puede usar el tiempo de vida por defecto del aviso del router ICMP (1800 segundos)

- El nodo móvil puede pedirle a un agente local que borre una unión particular de movilidad, mediante el envío de una solicitud de registro con la dirección temporal para este acople, con el campo de tiempo de vida colocado en cero.
- De manera similar, un tiempo de vida de cero se usa cuando el nodo móvil desregistra todas las direcciones temporales, aquellas sobre el regreso a su hogar.

El campo de dirección local debe estar configurado con la dirección local del nodo móvil, si esta información se conoce. De lo contrario, la dirección local debe colocarse en ceros.

El campo de dirección local debe estar configurado con la dirección del agente local del nodo móvil, si el nodo móvil conoce esta dirección. De lo contrario, el nodo móvil puede usar resolución dinámica de dirección del agente local, para aprender la dirección de su agente local. En este caso el nodo móvil debe colocar el campo de agente local con la dirección broadcast dirigida de subred, de la red local del nodo móvil. Cada agente local recibiendo tal solicitud de registro con una dirección de destino broadcast debe rechazar el registro del nodo móvil y debería regresar una respuesta de rechazo de registro, indicando su dirección IP unicast, para que el nodo móvil la use en un intento futuro de registro.

El campo de dirección temporal, debe ser colocado en el valor de la dirección temporal particular, que el nodo móvil desea para (des)registrarse. En el caso especial en el que el nodo móvil desea desregistrar todas las direcciones temporales, él debe configurar este campo con su dirección local.

El nodo móvil escoge el campo de identificación, de acuerdo con el estilo de protección de repeticiones que usa con su agente local. Esto es parte de la asociación de seguridad de movilidad que el nodo móvil comparte con su agente local. El método mediante el cual el nodo móvil computa el campo de identificación se encuentra en una sección posterior.

- ❖ Extensiones

Esta sección describe el orden de cualquier extensión obligatoria y de cualquier extensión opcional que un nodo móvil tiene como apéndice en una solicitud de registro. Este orden es REQUERIDO:

a. El encabezado IP, seguido por el encabezado UDP, seguido por la porción de longitud fija de la solicitud de registro, seguido por
b. Si está presente, cualquier extensión de no autenticación esperada para ser usada por el agente local u otro agente que autoriza (el cual puede o no puede también ser útil para el agente externo), seguida por
c. Todas las extensiones de habilitación de autorización, seguidas por
d. Si está presente, cualquier extensión de no autenticación utilizada solo por el agente externo, seguida por
e. La extensión de autenticación móvil-externa, si está presente.

Note que los ítems (a) y (c) deben aparecer en toda solicitud de registro enviada por el nodo móvil. Los ítems (b), (d) y (e) son opcionales. Sin embargo, el ítem (e) debe estar incluido cuando el nodo móvil y el agente externo comparten una asociación de seguridad de movilidad.

4.6.2 Recibiendo Respuestas de Registro. Las respuestas de registro serán recibidas por el nodo móvil como respuesta a sus solicitudes de registro. Las respuestas de registro generalmente están dentro de tres categorías:

- El registro fue aceptado.
- El registro fue denegado por el agente externo, o
- El registro fue denegado por el agente local.

El resto de esta sección describe el manejo de la respuesta de registro por un nodo móvil en cada una de estas categorías.

❖ Chequeo de Validez

Las respuestas de registro con una checksum UDP no-cero inválidas, deben ser descartadas silenciosamente.

Además, los 32 bits de bajo orden del campo de identificación en la respuesta de registro, deben ser comparados con los 32 bits de bajo orden del campo de identificación, en la solicitud de registro más reciente enviada al agente que responde. Si no coinciden, la respuesta debe ser descartada silenciosamente.

También, la respuesta de registro debe ser chequeada para la presencia de una extensión de habilitación de autorización. Para todos los mensajes de respuesta de registro, que contienen un código de estado indicando estado del agente local, el nodo móvil debe chequear la presencia de una extensión de

habilitación de autorización, actuando de acuerdo con el campo de código en la respuesta. Las reglas son:

a) Si el nodo móvil y el agente externo comparten una asociación de seguridad de movilidad, exactamente una extensión de autenticación móvil-externa debe estar presente en la respuesta de registro y el nodo móvil debe chequear el valor que autentica en la extensión. Si no se encuentra extensión de autenticación móvil-externa, o si se encuentra más de una extensión de autenticación móvil-externa, o si el autenticador es inválido, el nodo móvil debe descartar silenciosamente la respuesta y debería registrar el evento como una excepción de seguridad.

b) Si el campo de código indica que el servicio es negado por el agente local, o si el campo de código indica que el registro fue aceptado por el agente local, exactamente una extensión de autenticación móvil-local debe estar presente en la respuesta de registro y el nodo móvil debe chequear el valor autenticador en la extensión. Si la respuesta de registro fue generada por el agente local pero no se encuentra extensión de autenticación móvil-local, o si se encuentra más de una extensión de autenticación móvil-local, o si el autenticador es inválido, el nodo móvil debe descartar silenciosamente la respuesta y debería registrar el evento como una excepción de seguridad.

Si el campo de código indica una falla de autenticación, en el agente externo o en el agente local, entonces es muy posible que cualquier autenticador en la respuesta de registro esté también en error. Esto podría pasar, Por ejemplo si el secreto compartido entre el nodo móvil y el agente local fuera configurado de forma equivocada. El nodo móvil debería registrar tales errores como excepciones de seguridad.

- ❖ Solicitud de Registro Aceptada

Si el campo de código indica que la solicitud ha sido aceptada, el nodo móvil debería configurar su tabla de enrutamiento de forma apropiada, para su punto actual de acople o de conexión.

Si el nodo móvil está regresando a su red local y esa red es una de aquellas que implementa ARP, el nodo móvil debe seguir los procedimientos descritos en una sección posterior con respecto a ARP, ARP proxy y ARP gratuito.

Si el nodo móvil se ha registrado en una red externa, este debería volverse a registrar antes de que expire el tiempo de vida de su registro. Tal como se describe en las secciones anteriores, para cada solicitud de registro pendiente, el nodo móvil debe mantener el tiempo de vida restante de este registro

pendiente, así como también el tiempo de vida original de la respuesta de registro. Cuando el nodo móvil recibe una respuesta de registro válida, el nodo móvil debe decrementar su visión del tiempo de vida restante del registro, en la cantidad por la cual el agente local decrementó el tiempo de vida solicitado originalmente. Este procedimiento es equivalente a que el nodo móvil inicie un temporizador para el tiempo de vida concedido en el momento en que envió la solicitud de registro, incluso aunque el tiempo de vida concedido no es conocido para el nodo móvil, hasta que la respuesta de registro es recibida. Desde que la solicitud de registro sea correctamente enviada antes que el agente local comience a temporizar el tiempo de vida de registro (también basado en el tiempo de vida concedido), este procedimiento asegura que el nodo móvil se volverá a registrar antes de que el agente local haga expirar el registro y lo borre, a pesar de los posibles retardos insignificantes en las transmisiones para la solicitud original y la respuesta original de registro, que comenzaron el conteo del tiempo de vida en el nodo móvil y su agente local.

❖ Solicitud de Registro Denegada

Si el campo de código indica que el servicio está siendo denegado, el nodo móvil debería registrar el error. En varios casos el nodo móvil puede ser capaz de “reparar” el error. Esto incluye:

- Código 69: (denegado por agente externo, tiempo de vida muy largo). En este caso, el campo de tiempo de vida en la respuesta de registro tendrá el valor máximo de tiempo de vida que ese agente externo está dispuesto a aceptar en cualquier solicitud de registro. El nodo móvil puede intentar registrarse con este mismo agente, usando un tiempo de vida en la solicitud de registro que debe ser menor o igual al valor especificado en la respuesta.
- Código 133: (denegado por agente local, identificación no se ajusta). En este caso, el campo de identificación en la respuesta de registro tendrá un valor que permite al nodo móvil sincronizarse con el agente local, basado en efecto, en el estilo de protección de repeticiones. El nodo móvil debe ajustar los parámetros que usa para computar el campo de identificación basado en la información en la respuesta de registro, antes de emitir cualquier solicitud de registro futura.
- Código 136: (denegado por agente local, dirección de agente local desconocida). Este código es regresado por un agente local cuando el nodo móvil está ejecutando resolución dinámica de dirección de agente local, como se describe en las secciones anteriores, en este caso, el campo de agente local dentro de la respuesta tendrá la dirección IP unicast del agente local que está regresando la respuesta. El nodo móvil puede entonces intentar registrarse con este agente local en futuras solicitudes de registro. Además, el nodo móvil debería ajustar los parámetros que usa para computar el campo de identificación, basado en el campo correspondiente en la respuesta de registro, antes de emitir cualquier solicitud de registro futura.

4.6.3 Retransmisión de Registro. Cuando no se ha recibido respuesta de registro dentro de un tiempo razonable, otra solicitud de registro puede ser transmitida. Cuando se usan secciones de tiempo, una nueva identificación de registro es escogida para cada retransmisión; así se cuenta como un nuevo registro. Cuando se usan nonces, la solicitud no respondida es retransmitida sin cambios; así la retransmisión no se cuenta como un nuevo registro. En este sentido, una retransmisión no requerirá que el agente local se resincronice con el nodo móvil por medio de la emisión de otro nonce en caso tal que la solicitud de registro (en vez de su respuesta de registro) sea refundida por la red.

El tiempo máximo hasta que una nueva solicitud de registro es enviada, no debería ser más grande que el tiempo de vida solicitado de la solicitud de registro. El valor mínimo debería ser lo suficientemente grande para tenerse en cuenta en el tamaño de los mensajes, dos veces el tiempo de viaje de vuelta para transmisiones hacia el agente local, y al menos unos 100 milisegundos adicionales para permitir el procesamiento de los mensajes antes de responder. El tiempo de viaje de vuelta para la transmisión hacia el agente local, será al menos tan largo como el tiempo requerido, para transmitir los mensajes a la velocidad del enlace del punto de conexión actual del nodo móvil. Algunos circuitos agregan otros 200 milisegundos de retardo en el tiempo de viaje de vuelta total hacia el agente local. El tiempo mínimo entre solicitudes de registro NO debe ser menor que un (1) segundo. Cada período de tiempo fuera de retransmisiones sucesivas, debería ser al menos dos veces el tiempo previo, tan largo como este sea menor que el máximo, como se especificó más atrás.

4.7 CONSIDERACIONES DEL AGENTE EXTERNO

El agente externo juega un papel mucho más pasivo en el registro de IP Móvil. Él retransmite las solicitudes de registro entre nodos móviles y agente locales, y, cuando da la dirección temporal, desencapsula datagramas para entregar al nodo móvil. Debería también enviar mensajes periódicos de aviso de agente, para avisar su presencia como se describe en las primeras secciones, si no es detectable por medios de capa de enlace.

Un agente externo NO debe transmitir una solicitud de registro, excepto cuando está retransmitiendo una solicitud de registro recibida de un nodo móvil, para el agente local del nodo móvil. Un agente externo NO debe transmitir una respuesta de registro, excepto cuando está retransmitiendo una respuesta de registro recibida de un agente local de un nodo móvil., o cuando está respondiendo a una solicitud de registro recibida de un nodo móvil, en el caso que el agente externo esté negando servicio para el nodo móvil. En particular,

un agente externo NO debe generar una solicitud o respuesta de registro porque un tiempo de vida de registro de nodo móvil ha expirado. Un agente externo TAMPOCO debe originar un mensaje de solicitud de registro, que pida el desregistro de un nodo móvil; sin embargo, este debe retransmitir solicitudes de desregistro válidas originadas por un nodo móvil.

4.7.1 Tablas de Configuración y de Registro. Cada agente externo debe ser configurado con una dirección temporal. Además, para cada registro pendiente o actual, el agente externo debe mantener una lista de visitas de entrada, conteniendo la siguiente información obtenida a partir de la solicitud de registro del nodo móvil:

- Dirección de origen de capa de enlace del nodo móvil.
- La dirección IP de origen (dirección local del nodo móvil) o su dirección temporal Co-located (ver descripción del bit “R” en las secciones iniciales)
- La dirección IP de destino (como se especifica más atrás)
- El puerto de origen UDP.
- La dirección de agente local.
- El campo de identificación.
- El tiempo de vida de registro solicitado, y
- El tiempo de vida restante del registro pendiente o actual.

Si la dirección local del nodo móvil es cero (0) en el mensaje de solicitud de registro, entonces, el agente externo debe seguir los procedimientos especificados en el RFC 2794. En particular, si el agente externo no puede manejar fichas de solicitudes de registro pendientes, con tal dirección local cero (0) para el nodo móvil, el agente externo debe regresar una respuesta de registro, con código indicando NONZERO_HOMEADDR_REQD.

El agente externo puede configurar un máximo número de registros pendientes que está dispuesto a mantener (típicamente 5). Los registros adicionales deberían entonces ser rechazados por el agente externo con el código 66. El agente externo puede borrar cualquier solicitud de registro pendiente después de que la solicitud ha estado pendiente por más de 7 segundos; en este caso, el agente externo debería rechazar la solicitud con el código 78 (tiempo fuera de registro).

Como con cualquier nodo en Internet, un agente externo puede también compartir asociaciones de seguridad de movilidad con otros nodos cualquiera. Cuando está retransmitiendo una solicitud de registro de un nodo móvil a su agente local, si el agente externo comparte una asociación de seguridad de movilidad con el agente local, él debe añadir una extensión de autenticación externa-local a la solicitud y debe chequear la extensión de autenticación

externa-local requerida en la respuesta de registro del agente local. De forma similar, cuando está recibiendo una solicitud de registro de un nodo móvil, si el agente externo comparte una asociación de seguridad de movilidad con el nodo móvil, él debe chequear la extensión de autenticación móvil-externa requerida en la solicitud y debe añadir una extensión de autenticación móvil-externa a la respuesta de registro hacia el nodo móvil.

4.7.2 Recibiendo Solicitudes de Registro. Si el agente externo acepta una solicitud de registro de un nodo móvil, él la chequea para estar seguro de que la dirección de agente local indicada no pertenece a ninguna interfase de red del agente externo. Sino, el agente externo entonces debe retransmitir la solicitud al agente local indicado. De lo contrario, si el agente externo niega la solicitud, él debe enviar una respuesta de registro hacia el nodo móvil con un código de rechazo apropiado, excepto en casos donde el agente externo podría ser requerido para enviar más de una negación por segundo hacia el mismo nodo móvil. Las siguientes secciones describen este comportamiento con más profundidad.

Si el agente externo ha configurado una de sus interfases de red con la dirección IP especificada por el nodo móvil como su dirección de agente local, el agente externo NO debe pasar la solicitud otra vez. Si el agente externo sirve como un agente local al nodo móvil, el agente externo sigue los procedimientos especificados en numerales siguientes en el presente capítulo. De lo contrario, si el agente externo no sirve al nodo móvil como un agente local, el agente externo rechaza la solicitud de registro con código TBD-IANA (Dirección de agente local inválida).

Si un agente externo recibe una solicitud de registro de un nodo móvil en su lista de visitantes, la lista de visitantes de entrada para el nodo móvil NO debería borrarse o modificarse, hasta que el agente externo reciba una respuesta de registro válida del agente local, con un código que indique éxito. El agente externo debe grabar la nueva solicitud de registro pendiente como una parte separada de la lista de visitantes de entrada existente para el nodo móvil. Si la solicitud de registro solicita desregistro, la lista de visitantes de entrada existente para el nodo móvil, NO debería ser borrada hasta que el agente externo haya recibido una respuesta de registro exitosa. Si la respuesta de registro indica que la solicitud (para registro y desregistro) fue denegada por el agente local, la lista de visitantes de entrada existente para el nodo móvil, NO debe modificarse como resultado de recibir la respuesta de registro.

- ❖ Chequeos de Validez

Las solicitudes de registro con una checksum UDP diferentes de cero inválidas, deben ser descartadas silenciosamente. Las solicitudes con bits diferentes de cero en los campos reservados, deben ser rechazadas con el código 70

(solicitud pobremente formada). Las solicitudes con el bit “D” colocado en cero, tiempo de vida diferente de cero, y especificando una dirección temporal no ofrecida por el agente externo, deben ser rechazadas con el código 77 (dirección temporal inválida).

También, la autenticación en la solicitud de registro debe ser chequeada. Si el agente externo y el nodo móvil comparten una asociación de seguridad de movilidad, exactamente una extensión de autenticación móvil-externa debe estar presente en la solicitud de registro, y el agente externo debe chequear el valor autenticador en la extensión. Si no se encuentra extensión de autenticación móvil-externa, o si se encuentra más de una extensión de autenticación móvil-externa, o si el autenticador es inválido, el agente externo debe descartar silenciosamente la solicitud y debería registrar el evento como una excepción de seguridad. El agente externo también debería enviar una respuesta de registro hacia el nodo móvil con el código 67.

- ❖ Pasando una Solicitud Válida hacia el Agente Local

Si el agente externo acepta la solicitud de registro del nodo móvil, debe retransmitir la solicitud al agente local del nodo móvil como se especifica en el campo de agente local de la solicitud de registro. El agente externo NO debe modificar ninguno de los campos comenzando con la porción fija de la solicitud de registro, hasta la extensión de autenticación móvil-local u otra extensión de autenticación suministrada por el nodo móvil, como una extensión de habitación de autorización para el agente local. De lo contrario, es muy probable que ocurra una falla de autenticación en el agente local. Además, el agente externo procede así:

- Debe procesar y remover cualquier extensión que no preceda ninguna extensión de habilitación de autorización.
- Debe agregar cualquiera de sus propias extensiones de no autenticación de relevancia al agente local, si aplica, y
- debe agregar la extensión de autenticación externa-local, si el agente externo comparte una asociación de seguridad de movilidad con el agente local.

Algunos campos específicos dentro del encabezado IP y el encabezado UDP de la solicitud de registro retransmitida, deben ser configurados de la siguiente forma:

- Dirección IP de origen: la dirección temporal ofrecida por el agente externo para el nodo móvil que envía la solicitud de registro.
- Dirección IP de destino: copiada del campo de agente local dentro de la solicitud de registro.

- Puerto UDP de origen: (variable).
- Puerto UDP de destino: 434.

Después de pasar una solicitud de registro válida al agente local, el agente externo debe comenzar a temporizar el tiempo de vida restante del registro pendiente, basado en el tiempo de vida en la solicitud de registro. Si este tiempo de vida expira antes de recibir una respuesta de registro válida, el agente externo debe borrar su lista de visitantes de entrada para este registro pendiente.

❖ Denegando Solicitudes Inválidas

Si el agente externo niega la solicitud de registro del nodo móvil por cualquier razón, debería enviarle al nodo móvil una respuesta de registro con un código adecuado de negación. En tal caso, la dirección local, el agente local y los campos de identificación dentro de la respuesta de registro, son copiados de los campos correspondientes de la solicitud de registro.

Si el campo reservado no es cero, el agente externo debe denegar la solicitud y debería regresar una respuesta de registro con un código de estado 70 hacia el nodo móvil. Si la solicitud está siendo denegada debido a que el tiempo de vida solicitado es muy largo, el agente externo coloca el tiempo de vida en la respuesta, en el valor máximo de tiempo de vida que está dispuesto a aceptar en cualquier solicitud de registro y coloca el campo de código en 69. De lo contrario, el tiempo de vida debería ser copiado del campo de tiempo de vida en la solicitud.

Algunos campos específicos dentro del encabezado IP y del encabezado UDP de la respuesta de registro deben ser configurados de la siguiente forma:

- Dirección IP de origen: copiada de la dirección IP de destino de la solicitud de registro, a no ser que “todas las direcciones multicast de los agentes” fueran usadas. En este caso, la dirección del agente externo (en la interfase desde la cual el mensaje será enviado), debe ser usada.
- Dirección IP de destino: si la respuesta de registro es generada por el agente externo con el objeto de rechazar una solicitud de registro del nodo móvil y la solicitud de registro contiene una dirección local la cual no es 0.0.0.0, entonces la dirección IP de destino es copiada del campo de dirección local de la solicitud de registro. De lo contrario, si la respuesta de registro es recibida desde el agente local y contiene una dirección local la cual no es 0.0.0.0, entonces la dirección IP de destino es copiada del campo de dirección local de la respuesta de registro. De otro modo, la dirección IP de destino de la respuesta de registro es configurada para que sea 255.255.255.255.

- Puerto UDP de origen: 434.
- Puerto UDP de destino: copiado del puerto UDP de origen de la solicitud de registro.

4.7.3 Recibiendo Respuestas de Registro. El agente externo actualiza su lista de visitantes, cuando recibe una respuesta de registro válida del agente local. Él retransmite entonces la respuesta de registro hacia el nodo móvil. Las siguientes secciones describen el comportamiento con más detalle.

Si sobre la retransmisión de una solicitud de registro hacia un agente local, el agente externo recibe un mensaje de error ICMP en lugar de una respuesta de registro, el agente externo entonces debería enviar hacia el nodo móvil una respuesta de registro, con un código de falla apropiada "Agente Local Inalcanzable" (dentro del rango 80-95). Los detalles de la construcción de la respuesta de registro se pueden consultar en las secciones inmediatamente anteriores.

❖ Chequeos de Validez

Las respuestas de registro con un checksum UDP inválido diferente de cero, deben ser descartadas silenciosamente.

Cuando un agente externo recibe un mensaje de respuesta de registro, debe buscar en su lista de visitantes, una solicitud de registro pendiente con la misma dirección local del nodo móvil, como se indica en la respuesta. Si no se encuentra tal solicitud pendiente y si la respuesta de registro no corresponde con alguna solicitud de registro pendiente con una dirección local cero de nodo móvil, el agente externo debe descartar silenciosamente la respuesta. El agente externo debe también descartar silenciosamente la respuesta, si los 32 bits de bajo orden del campo de identificación en la respuesta, no concuerdan con los de la solicitud.

También, la autenticación en la respuesta de registro debe ser revisada. Si el agente externo y el agente local comparten una asociación de seguridad de movilidad, exactamente una extensión de autenticación externa-local debe estar presente en la respuesta de registro y el agente externo debe chequear el valor autenticador en la extensión. Si no se encuentra extensión de autenticación externa-local o si se encuentra más de una extensión de autenticación externa-local o si el autenticador es inválido, el agente externo debe descartar silenciosamente la respuesta y debería registrar el evento como una excepción de seguridad. El agente externo también debe rechazar el registro del nodo móvil y debería enviar una respuesta de registro hacia el nodo móvil con código 68.

❖ Pasando Respuestas hacia el Nodo Móvil

Una respuesta de registro que satisface los chequeos de validez descrita en secciones posteriores, es retransmitida hacia el nodo móvil. El agente externo debe también actualizar su lista de entrada de visitantes para que el nodo móvil refleje los resultados de la solicitud de registro, como se indica por el campo de código en la respuesta. Si el código indica que el agente local ha aceptado el registro y el campo de tiempo de vida no es cero, el agente externo debería configurar el tiempo de vida en la lista de entrada de visitantes en el mínimo de los siguientes valores:

- El valor especificado en el campo de tiempo de vida de la respuesta de registro, y
- El máximo valor propio del agente externo, para el tiempo de vida de registro admisible.

Si por el contrario, el código indica que el campo de tiempo de vida es cero, el agente externo debe borrar su lista de entrada de visitantes para el nodo móvil. Finalmente, si el código indica que el registro fue denegado por el agente local, el agente externo debe borrar su lista de entrada de registros pendientes, pero no su lista de entrada de visitantes, para el nodo móvil.

El agente externo NO debe modificar ninguno de los campos comenzando con la porción fija de la respuesta de registro, hasta la extensión de autenticación móvil-local inclusive. De lo contrario, es muy probable que ocurra una falla de autenticación en el nodo móvil. Además, el agente externo debería ejecutar los siguientes procedimientos adicionales:

- Debe procesar y remover cualquier extensión que no está cubierta por una extensión de habilitación de autorización.
- Debe añadir sus propias extensiones de no autenticación, que suministran información al nodo móvil, si es aplicable, y
- debe añadir la extensión de autenticación móvil-externa, si el agente externo comparte una asociación de seguridad de movilidad con el nodo móvil.

Campos específicos dentro del encabezado IP y dentro del encabezado UDP de la respuesta de registro retransmitida, son configurados de acuerdo con las mismas reglas especificadas en secciones anteriores.

Después de pasar una respuesta de registro válida al nodo móvil, el agente externo debe actualizar su lista de visitantes de entrada para este registro

como sigue. Si la respuesta de registro indica que el registro fue aceptado por el agente local, el agente externo reconfigura su temporizador del tiempo de vida del registro, al tiempo de vida concedido en la respuesta de registro; a diferencia del conteo de tiempo del nodo móvil del tiempo de vida de registro, como se describe en antes, el agente externo considera este tiempo de vida para comenzar cuando pasa el mensaje de respuesta de registro, asegurando que el agente externo no hará expirar el registro antes que el nodo móvil lo haga. Por otro lado, si la respuesta de registro indica que el registro fue rechazado por el agente local, el agente externo borra su lista de visitantes de entrada para este intento de registro.

4.8 CONSIDERACIONES DE AGENTE LOCAL

Los agente locales juegan un papel reactivo en el proceso de registro. El agente local recibe solicitudes de registro del nodo móvil (tal vez retransmitido por un agente externo), actualiza su historia de conexiones de movilidad para este nodo móvil y emite una respuesta de registro apropiada en respuesta a cada uno.

Un agente local NO debe transmitir una respuesta de registro, excepto cuando se responde a una solicitud de registro recibida de un nodo móvil. De forma particular, el agente local NO debe generar una respuesta de registro para indicar que el tiempo de vida ha expirado.

4.8.1 Tablas de Configuración y de Registro. Cada agente local debe estar configurado con una dirección IP y con el prefijo de tamaño para la red local. El agente local debe estar configurado con la asociación de seguridad de movilidad de cada nodo móvil autorizado, que está sirviendo como un agente local.

Cuando el agente local acepta una solicitud de registro válida de un nodo móvil que sirve como un agente local, el agente local debe crear o modificar la entrada para este nodo móvil, en su lista de vínculos de movilidad, que contiene:

- La dirección local del nodo móvil.
- La dirección temporal del nodo móvil.
- El campo de identificación de la respuesta de registro.
- El tiempo de vida restante del registro.

El agente local puede opcionalmente ofrecer la capacidad de asociar dinámicamente una dirección local a un nodo móvil, al recibir una solicitud de registro de ese nodo móvil. El método mediante el cual una dirección local es asignada al nodo móvil no es objeto del trabajo. Después de que el agente local hace la asociación de la dirección local al nodo móvil, el agente local debe poner esa dirección dentro del campo de dirección local de la respuesta de registro.

El agente local puede también mantener asociaciones de seguridad de movilidad con varios agentes externos. Cuando se recibe una solicitud de registro de un agente externo, si el agente local comparte una asociación de seguridad de movilidad con el agente externo, el agente local debe revisar el autenticador en la extensión de autenticación externa-local en el mensaje, basado en esta asociación de seguridad de movilidad. De manera similar, cuando se envía una respuesta de registro a un agente externo, si el agente local comparte una asociación de seguridad de movilidad con el agente externo, el agente local debe incluir una extensión de autenticación externa-local en el mensaje, basado en esta asociación de seguridad de movilidad.

4.8.2 Recibiendo Solicitudes de Registro. Si el agente local acepta una solicitud de registro entrante, debe actualizar su historia del (los) vínculo(s) de movilidad del nodo móvil y debería enviar una respuesta de registro con un código adecuado. De lo contrario (el agente local niega la solicitud), él debería enviar una respuesta de registro con un código apropiado, especificando la razón por la cual la solicitud fue denegada. Las siguientes secciones describen este comportamiento con mayor profundidad. Si el agente local no soporta broadcasts él debe ignorar el bit “B” (a diferencia de la solicitud de registro rechazada).

- ❖ Chequeos de Validez

Las solicitudes de registro con un checksum UDP inválido diferente de cero, deben ser descartadas silenciosamente por el agente local.

La autenticación en la solicitud de registro debe ser revisada. Esto implica las siguientes operaciones:

a) El agente local debe chequear la presencia de al menos una extensión de habilitación de autorización y asegurar que todas las autenticaciones indicadas son llevadas a cabo. Al menos una extensión de habilitación de autenticación debe estar presente en la solicitud de registro; y el agente local debe verificar el valor autenticador en la extensión o verificar que el valor autenticador ha sido revisado por otro agente con el cual él tiene una asociación de seguridad. Si no se encuentra extensión de habilitación de

autenticación o si el autenticador es inválido, el agente local debe rechazar el registro del nodo móvil y debería enviar una respuesta de registro hacia el nodo móvil con el código 131. El agente local debe entonces descartar la solicitud y debería registrar el error como una excepción de seguridad. Si el agente local recibe una solicitud de registro sin una extensión de autenticación móvil-local, de un nodo móvil que tiene una asociación de seguridad con este agente local, el agente local debe descartar la solicitud de registro del nodo móvil.

b) El agente local debe chequear que el campo de identificación de registro es correcto, usando el contexto seleccionado por el SPI dentro de la extensión de habilitación de autorización, que el agente local usó para autenticar la solicitud de registro del nodo móvil. Para una descripción de cómo se hace esto se puede ir a secciones siguientes. Si es incorrecto, el agente local debe rechazar la solicitud y debería enviar una respuesta de registro al nodo móvil con el código 133, incluyendo un campo de identificación, computado de acuerdo con las reglas especificadas más adelante el agente local no debe hacer procesamiento adicional con aquella solicitud, aunque debería registrar el error como una excepción de seguridad.

c) Si el agente local comparte una asociación de seguridad de movilidad con el agente externo, y esta solicitud de registro (tiene tiempo de vida diferente de cero), el agente local debe chequear la presencia de una extensión de autenticación externa-local. Exactamente, debe estar presente una extensión de autenticación externa-local en la solicitud de registro en este caso, y el agente local debe chequear el valor autenticador en la extensión. Si no se encuentra extensión de autenticación externa-local, o si se encuentra más de una extensión de autenticación externa-local, o si el autenticador es inválido, el agente local debe rechazar el registro del nodo móvil y debería enviar una respuesta de registro hacia el nodo móvil con código 132. El agente local debe entonces descartar la solicitud y debería registrar el error como una excepción de seguridad.

Además, para chequear la autenticación en la solicitud de registro, los agentes locales deben denegar solicitudes de registro, que son enviadas hacia la dirección broadcast dirigida de subred de la red local (en vez de ser unicast hacia el agente local). El agente local debe descartar la solicitud y debería regresar una respuesta de registro con un código de 136. En este caso, la respuesta de registro contendrá la dirección unicast del agente local, de tal manera que el nodo móvil puede re-emitir la solicitud de registro con la dirección correcta de agente local.

Nótese que algunos routers cambian la dirección IP de destino de un datagrama, de una dirección broadcast dirigida de subred a 255.255.255.255,

antes de colocarlo en la subred de destino. En este caso, los agentes locales que intentan tomar solicitudes dinámicas de descubrimiento de agente local, por medio del vínculo de un socket, explícitamente a la dirección broadcast dirigida de subred, no verán tales paquetes. Los implementadores del agente local deberían estar preparados tanto para las direcciones broadcast dirigidas de subred y para 255.255.255.255, si ellos desean soportar descubrimiento de agente local dinámico.

❖ Aceptando una Solicitud Válida

Si la respuesta de registro satisface los Chequeos de validez, y el agente local es capaz de acomodar la solicitud, el agente local debe actualizar su lista de vínculos de movilidad para el nodo móvil solicitante y debe regresar una respuesta de registro al nodo móvil. En este caso, el código de respuesta será cero (0) si el agente local soporta vínculos de movilidad simultáneos, o uno (1) si no los soporta. Para detalles acerca de la construcción del mensaje de respuesta de registro se pueden consultar secciones siguientes.

El agente local actualiza su archivo de los vínculos de movilidad del nodo móvil como sigue, basado en los campos en la solicitud de registro:

- Si el tiempo de vida es cero y la dirección temporal iguala la dirección local del nodo móvil, el agente local borra todas las entradas en la lista de vínculos de movilidad para el nodo móvil solicitante. Así es como el nodo móvil solicita que su agente local pare de brindar servicios de movilidad.
- Si el tiempo de vida es cero y la dirección temporal no iguala la dirección local del nodo móvil, el agente local borra únicamente la entrada que contiene la dirección temporal especificada, de la lista de vínculos de movilidad para el nodo móvil solicitante. Cualquier otra entrada activa que contiene otra dirección temporal permanecerá activa.
- Si el tiempo de vida es diferente de cero, el agente local agrega una entrada que contiene la dirección temporal solicitada a la lista de vínculos de movilidad para el nodo móvil. Si el bit “S” está colocado y el agente local soporta vínculos de movilidad simultáneos, las entradas anteriores de vínculos de movilidad se mantienen. De lo contrario, el agente local remueve todas las entradas previas en la lista de vínculos de movilidad para el nodo móvil.

En todos los casos, el agente local debe enviar una respuesta de registro a la fuente de la solicitud de registro, la cual debe ser verdaderamente un agente externo diferente de aquel cuya dirección temporal está siendo (des)registrada. Si el agente local comparte una asociación de seguridad de movilidad con el agente externo, cuya dirección temporal está siendo desregistrada, y ese agente externo es diferente del que relevó la solicitud de registro, el agente local puede enviar adicionalmente una respuesta de registro al agente externo,

cuya dirección temporal está siendo desregistrada. El agente local NO debe enviar tal respuesta si no comparte una asociación de seguridad de movilidad con el agente externo. Si no se envía respuesta, la lista de visitantes del agente externo caducará naturalmente cuando el tiempo de vida original expire.

Un desregistro el cual pasa a través de un agente externo, el cual es diferente de aquel cuya dirección temporal está siendo desregistrada, puede añadir una extensión de autenticación externa-local a ese desregistro. Sin embargo, como este desregistro concierne a un agente externo diferente de aquel de la extensión de autenticación, el agente local debe pasar por alto la extensión de autenticación externa-local de tal desregistro. Los chequeos de validez restantes descritos antes, son necesarios en su totalidad.

El agente local NO debe incrementar el tiempo de vida por encima de lo especificado por el nodo móvil en la solicitud de registro. Sin embargo, no es un error para el nodo móvil solicitar un tiempo de vida más largo del que el agente local está dispuesto a aceptar. En este caso, el agente local simplemente reduce el tiempo de vida a un valor permisible y regresa este valor en la respuesta de registro. El valor del tiempo de vida en la respuesta de registro, informa al nodo móvil del tiempo de vida concedido del registro, indicándole cuando debería re-registrarse con el objetivo de mantener servicio continuo. Después de la expiración de este tiempo de vida de registro, el agente local debe borrar su entrada para este registro en la lista de vínculos de movilidad. Si la solicitud de registro duplica una actual solicitud de registro aceptada, el nuevo tiempo de vida NO debe extenderse más del tiempo de vida originalmente concedido. Una solicitud de registro es un duplicado si la dirección local, la dirección temporal y los campos de identificación, son todos iguales a los de un registro actual aceptado.

Además, si la red local implementa ARP, la solicitud de registro pide que el agente local cree un vinculo de movilidad para un nodo móvil, el cual previamente no tenía vínculo (se asumió previamente que el nodo móvil estaba en su casa), entonces el agente local debe seguir los procedimientos descritos en una sección más adelante con respecto a ARP, ARP Proxy y ARP gratuito. Si el nodo móvil ya tuvo un vínculo de movilidad previo, el agente local debe continuar siguiendo las reglas para ARP Proxy descritas posteriormente.

- ❖ Denegando Una Solicitud Inválida

Si la solicitud de registro no satisface la totalidad de los chequeos de validez, o el agente local no es capaz de acomodar la solicitud, el agente local debería regresar una respuesta de registro hacia el nodo móvil con un código que indique la razón del error. Si un agente externo fue involucrado en el reenvío de la solicitud, esto permite al agente externo borrar su lista de entrada de

visitantes pendiente. También, esto informa al nodo móvil de la razón del error, tal que puede intentar fijar el error y emitir otra solicitud.

Esta sección muestra un número de razones por las que el agente debe rechazar una solicitud, y provee el valor de código que él debería usar en cada instancia. Para detalles adicionales acerca de la construcción del mensaje de respuesta de registro, se pueden consultar las secciones siguientes que tratan el tema.

Muchas razones por las cuales rechazar un registro son administrativas en esencia. Por ejemplo, un agente puede limitar el número de registros simultáneos para un nodo móvil, mediante el rechazo de todos los registros que causarían que su límite se exceda, y regresando una respuesta de registro con código de error 135. De manera similar, un agente local puede negarse a conceder servicio a nodos móviles que hayan ingresado a áreas de servicio no autorizadas, mediante una respuesta de registro con código 129.

Solicitudes con bits diferentes de cero en los campos reservados, deben ser rechazadas con el código 134 (solicitudes formadas pobremente).

4.8.3 Enviando Respuestas de Registro. Si el agente local acepta una solicitud de registro, este debe entonces actualizar su historial del(los) vínculo(s) de movilidad del nodo móvil y debería enviar una respuesta de registro con un código adecuado. De lo contrario (el agente local ha denegado la solicitud), este debería enviar una respuesta de registro con un código apropiado, especificando la razón por la cual la solicitud fue denegada. Las siguientes secciones proveen detalles adicionales para los valores que el agente local debe suministrar en los campos de los mensajes de respuesta de registro.

- Campos IP/UDP

Esta sección brinda las reglas específicas por las cuales los agentes locales toman valores para los campos de encabezado IP y UDP de una respuesta de registro.

Dirección IP de origen: copiada de la dirección IP de destino de la solicitud de registro, a menos que una dirección multicast o broadcast sea utilizada. Si la dirección IP de destino de la solicitud de registro fue una dirección multicast o broadcast, la dirección IP de origen de la respuesta de registro debe ser configurada con la dirección IP (unicast) del agente local.

Dirección IP de destino: copiada de la dirección IP de origen de la solicitud de registro.

Puerto UDP de origen: copiado del puerto UDP de destino de la solicitud de registro.

Puerto UDP de destino: copiado del puerto UDP de origen de la solicitud de registro.

Cuando se envía una respuesta de registro, como respuesta a una solicitud de registro que solicitó desregistro del nodo móvil (el tiempo de vida es cero y la dirección temporal iguala la dirección local del nodo móvil) y en la cual la dirección IP de origen fue también colocada con la dirección local del nodo móvil (este es el método normal usado por el nodo móvil para desregistrarse cuando retorna a su red local), la dirección IP de destino en la respuesta de registro será colocada con la dirección local del nodo móvil, como copiada de la dirección IP de origen de la solicitud.

En este caso, cuando se transmite la respuesta de registro, el agente local debe transmitir la respuesta directamente sobre la red local, como si el nodo móvil estuviera en casa, evitando toda lista de entrada de vínculos de movilidad que puedan existir todavía en el agente local, para el nodo móvil de destino. En particular, para que el regreso a casa del nodo móvil después de estar registrado con una dirección temporal, si la nueva solicitud de registro del nodo móvil no es aceptada por el agente local, la lista de entrada de vínculos de movilidad para el nodo móvil aún indicará que los datagramas direccionados hacia el nodo móvil, deberían ser enviados por túneles, hacia la dirección temporal registrada del nodo móvil; cuando se envía la respuesta de registro indicando el rechazo de esta solicitud, esta lista de entrada de vínculos existentes debe ser ignorada, y el agente local debe transmitir esta respuesta como si el nodo móvil estuviera en casa.

- ❖ Campos de Respuesta de Registro

Esta sección ofrece las reglas específicas por las cuales, los agentes locales toman valores para los campos, dentro de la porción fija de una respuesta de registro.

El campo Código de la respuesta de registro es escogido de acuerdo con las reglas especificadas en las secciones anteriores. Cuando se contesta a un registro aceptado, un agente local debería responder con código 1 si este no soporta registros simultáneos.

El campo Tiempo de vida debe ser copiado del correspondiente campo en la solicitud de registro, a menos que el valor solicitado sea más grande que la longitud máxima del tiempo que el agente local espera brindar el servicio solicitado. En tal caso, el Tiempo de vida debe ser colocado con la longitud de tiempo, que el servicio será brindado realmente por el agente local. Este Tiempo de vida reducido, debería ser el tiempo de vida máximo permitido por el agente local (para este nodo móvil y dirección temporal).

Si el campo de Dirección Local de la solicitud de registro es diferente, no es cero, este debe ser copiado en el campo de Dirección Local del mensaje de respuesta de registro. Si el agente local no puede soportar la dirección unicast especificada diferente de cero en el campo de Dirección Local de la solicitud de registro, entonces el agente local debe rechazar la solicitud de registro con un código de error de 129.

De lo contrario, si el campo de Dirección Local de la solicitud de registro es cero, como se especifica en una sección anterior, el agente local debería arreglar la selección de una dirección local para el nodo móvil, e insertar la dirección seleccionada en el campo de Dirección Local del mensaje de respuesta de registro. Hay detalles relevantes más avanzados en el caso donde los nodos móviles se identifican a si mismos usando una NAI, en lugar de su dirección IP local.

Si el campo de Agente Local en la solicitud de registro contiene una dirección unicast de este agente local, entonces ese campo debe ser copiado en el campo de Agente Local de la respuesta de registro. De lo contrario, el agente local debe colocar el campo de Agente Local en la respuesta de registro con su dirección unicast. En este último caso, el agente local debe rechazar el registro con un código adecuado (por ejemplo código 136) para evitar que el nodo móvil sea registrado simultáneamente con dos o más agentes locales.

- ❖ Extensiones

Esta sección describe el orden de cualquier Extensión de IP Móvil requerida u opcional, que un agente local añade a una respuesta de registro. Se debe seguir el siguiente orden.

a) El encabezado IP, seguido por el encabezado UDP, seguido por la porción de longitud fija de la respuesta de registro.
b) Si esta presente, cualquier extensión de no autenticación utilizada por el nodo móvil (la cual puede o no puede ser usada también por el agente externo)
c) La extensión de autenticación móvil-local.

d) Si se presenta, cualquier extensión de no autenticación utilizada solo por el agente externo, y
e) La extensión de autenticación externa-local, si se presenta.

Note que los ítems a) y c) deben aparecer en toda respuesta de registro enviada por el agente local. Los ítems b), d) y e) son opcionales. Sin embargo, el ítem e) debe ser incluido cuando el agente local y el agente externo comparten una asociación de seguridad de movilidad.

5. CONSIDERACIONES DE ENRUTAMIENTO

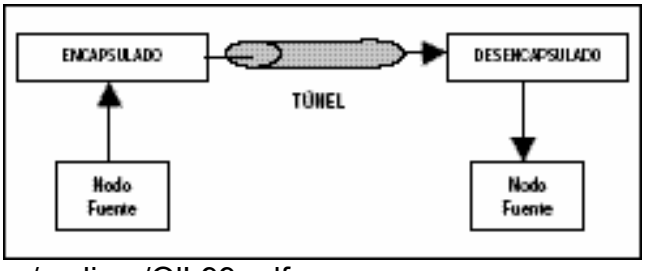
Esta sección describe como los nodos móviles, los agentes locales y (posiblemente) los agentes externos cooperan para enrutar datagramas hacia / desde nodos móviles que están conectados a una red externa. El nodo móvil informa a su agente local de su localización actual utilizando el procedimiento de registro descrito en el capítulo anterior. Para sitios relativos de la dirección local del nodo móvil con respecto a su agente local, y el nodo móvil como tal con respecto a cualquier agente externo con el que puede intentar registrarse, se puede consultar la sección de Visión general del protocolo.

5.1 TIPOS DE ENCAPSULAMIENTO

Los agentes locales y los agentes externos deben soportar datagramas enviados por túnel usando IP en encapsulamiento IP. Cualquier nodo móvil que use una dirección temporal Co-located debe soportar datagramas que se reciben, enviados por túneles utilizando IP en encapsulamiento IP. El encapsulamiento mínimo y el encapsulamiento GRE son métodos alternativos de encapsulamiento que pueden de manera opcional ser soportados por agentes de movilidad y nodos móviles. El uso de estas formas alternativas de encapsulamiento, cuando se solicita por el nodo móvil, está por el contrario a discreción del agente local.

“El término encapsulado o encapsulamiento es un equivalente al de tunneling. Este consiste en la inserción de un paquete IP dentro de otro paquete del mismo tipo o diferente. El paquete resultante es , enviado a continuación, a un nodo intermedio entre el nodo origen y el nodo final. El escenario más común de utilización de túneles es el que se muestra en la figura 27.

Figura 27. Tunneling



http://acimut.upf.es/moliver/OIL99.pdf

El nodo encapsulador es normalmente considerado el punto de entrada al túnel y el nodo desencapsulador, el punto de salida del túnel. Hoy en día las técnicas de encapsulamiento IP son muy útiles para realizar transmisiones *multicast*, e incluso para llevar a cabo acciones de seguridad y privacidad en Internet.

El protocolo IP Móvil necesita que los agentes locales, los agentes externos y los nodos móviles con una dirección temporal Co-located soporten el *encapsulado IP-en-IP*. En esta sección se presentan éste y otros tipos de encapsulamiento que el agente local puede emplear para enviar los paquetes a través de túneles, con el objeto de entender un poco mejor el proceso de reenvío de paquetes.

El encapsulado IP-en-IP consiste en introducir una cabecera IP adicional, antes de la cabecera propia del paquete original, similar a como se muestra en la figura 28. También es posible introducir otras cabeceras (como por ejemplo, requisitos de seguridad para proteger el paquete original durante el proceso de tunneling) entre las dos cabeceras previas.

La cabecera exterior tiene información sobre los extremos del túnel. La cabecera interna tiene información sobre los nodos origen y destino del paquete original y no puede ser modificada de ninguna manera, excepto para decrementar el tiempo de vida (TTL - Time To Live) del paquete, aunque tan solo una vez dentro del túnel, a pesar de que pueda pasar por varios routers.

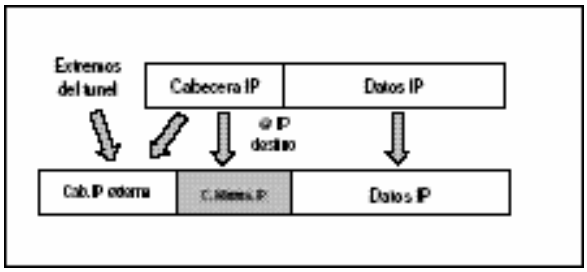
A simple vista podría parecer que resulta imposible saber si se ha producido algún inconveniente con el paquete, mientras éste se encuentra dentro del túnel. Sin embargo, el punto de entrada al túnel mantiene varias informaciones, compuestas por un juego de variables que describen las características del túnel. Esta información está formada por:

- Máxima MTU (Maximum Transfer Unit) del túnel.
- Longitud del túnel, contabilizada en saltos de router o nodos.
- Si el extremo final del túnel es alcanzable, el punto de entrada al túnel actualiza estas variables mediante mensajes ICMP que recibe de los routers en el interior del túnel.

El encapsulamiento suele conllevar el duplicado innecesario de numerosos campos de la cabecera IP interna. El encapsulamiento mínimo intenta minimizar al máximo la información de *overhead* de encapsulamiento, para disminuir el tamaño del paquete resultante. Según puede como se muestra en la figura 28, la cabecera IP original es modificada y la cabecera de

encapsulamiento mínimo es insertada entre la cabecera original modificada y la información.

Figura 28. Encapsulamiento mínimo



http://acimut.upf.es/moliver/OIL99.pdf

Al desencapsular un paquete con encapsulamiento mínimo, se deberán restaurar los campos modificados en la cabecera original con los datos de la cabecera de encapsulamiento mínimo, actualizando los campos que así lo requieran, como por ejemplo el campo de longitud del paquete y el de checksum.

A pesar de todo, el encapsulamiento mínimo no está ampliamente difundido ya que muestra ciertas desventajas. Específicamente, no funciona con paquetes ya fragmentados. Además, este encapsulamiento fuerza que el valor TTL sea decrementado en cada router dentro del túnel, por lo que puede suceder que los paquetes expiren antes de llegar a su destino.

El encapsulado *GRE (*Generic Record Encapsulation*)* es el más flexible los tres estudiados posibles, ya que permite la encapsulación de cualquier tipo de paquete, incluidos los paquetes IP. El formato del paquete GRE es el que se puede ver en la figura 29.

Figura 29. Encapsulamiento GRE

http://acimut.upf.es/moliver/OIL99.pdf

Contrario a los encapsulamientos IP-en-IP y mínimo, el encapsulado GRE ha sido diseñado para prevenir encapsulamientos recursivos. De manera

específica, el campo recur en la cabecera es un contador que informa sobre el número de encapsulamientos adicionales que son permitidos. "[3]

5.2 ENRUTAMIENTO DE DATAGRAMAS UNICAST

5.2.1 Consideraciones de Nodo Móvil. Cuando esta conectado a su red local, un nodo móvil opera sin el soporte de servicios de movilidad. Esto es, él opera de la misma forma como cualquier otro host o router (fijo). El método mediante el cual un nodo móvil selecciona un router por defecto cuando está conectado a su red local, o cuando está lejos de casa y utilizando una dirección temporal Co-located, hace parte de un estudio más detallado el cual no se incluye en este documento. El aviso de router ICMP implica tal método.

Cuando está registrado sobre una red externa, el nodo móvil escoge un router por defecto mediante las siguientes reglas:

- Si el nodo móvil está registrado usando una dirección temporal de agente externo, este debe usar a su agente externo como el primer salto de router. La dirección MAC del agente externo puede ser aprendida a partir del aviso de agente. De lo contrario, el nodo móvil debe escoger su router por defecto de entre las direcciones de router avisadas, en la porción del aviso de router ICMP de ese mensaje de aviso de agente.
- Si el nodo móvil está registrado directamente con su agente local usando una dirección temporal co-located, entonces el nodo móvil debería escoger su router por defecto de entre aquellos avisados en cualquier mensaje de aviso de router ICMP que él recibe, por los cuales su dirección temporal obtenida externamente y la dirección de router se ajustan bajo el prefijo de red. Si la dirección temporal obtenida externamente del nodo móvil se ajusta a la dirección IP de origen del aviso de agente bajo el prefijo de red, el nodo móvil puede también considerar a esa dirección IP de origen, como otra opción posible para la dirección IP de un router por defecto. El prefijo de red puede ser obtenido a partir de la extensión de longitudes prefijas en el aviso de router ICMP, si está presente. El prefijo también puede ser obtenido a través de otros mecanismos que no se describen por razones de limitación del tema.

Mientras que están fuera de la red local, los nodos móviles NO deben enviar paquetes ARP broadcast para encontrar la dirección MAC de otro nodo de Internet. Así, la lista de direcciones de router (posiblemente vacía) de la porción

[3] Aparte de la sección de Encapsulado del documento Mobile IP: una solución para proporcionar movilidad de los terminales en Internet. [Documento en Línea]. 2004. Disponible en Internet < http://acimut.upf.es/moliver/OlL99.pdf >

de aviso de router ICMP del mensaje, no es útil para seleccionar un router por defecto, a menos que el nodo móvil tenga algunos medios que no involucren ARP broadcast y no especificados dentro de este documento, para la obtención de la dirección MAC de uno de los routers en la lista. De manera similar, en ausencia de mecanismos no especificados para obtener direcciones MAC en redes externas, el nodo móvil debe ignorar redireccionamientos hacia otros routers sobre redes externas.

5.2.2 Consideraciones de Agente Externo. Sobre el recibo de un datagrama encapsulado a su dirección temporal avisada, un agente externo debe comparar la dirección de destino interna con aquellas entradas en su lista de visitantes. Cuando el destino no encaja con la dirección de cualquier nodo móvil actualmente en la lista de visitantes, el agente externo NO debe pasar el datagrama sin modificaciones al encabezado IP original, porque de lo contrario es probable que resulte un bucle de enrutamiento. El datagrama debería ser descartado silenciosamente. NO debe ser enviado Destino ICMP Inalcanzable, cuando un agente externo no es capaz de pasar un datagrama entrante enviado por túnel. De otra forma, el agente externo pasa el datagrama desencapsulado hacia el nodo móvil.

El agente externo NO debe avisar a otros routers en su dominio de enrutamiento, ni a ningún otro nodo móvil, la presencia de un router móvil o nodo móvil en su lista de visitantes.

El agente externo debe enrutar datagramas que recibe desde nodos móviles registrados. Como mínimo, esto significa que el agente externo debe verificar el Checksum del encabezado IP, decrementar el Tiempo de vida IP, recomputar el Checksum del encabezado IP, y pasar hacia delante tales datagramas hacia un router por defecto.

Un agente externo NO debe usar ARP broadcast para una dirección MAC del nodo móvil sobre una red externa. Él puede obtener la dirección MAC copiando la información de una solicitud de agente o una Solicitud de registro transmitida desde un nodo móvil. Una cache ARP de agente externo para la dirección IP del nodo móvil NO debe ser permitida para que expire antes que la lista de visitantes de entrada del nodo móvil expire, a menos que el agente externo tenga alguna otra manera fuera de ARP broadcast, para refrescar su dirección MAC asociada con la dirección IP del nodo móvil.

Cada agente externo debería soportar los rasgos obligatorios para Tunneling en sentido contrario.

5.2.3 Consideraciones de Agente Local. El agente local debe ser capaz de interceptar cualquier datagrama sobre la red local, direccionado hacia el nodo móvil, mientras el nodo móvil esté registrado fuera de su casa. ARP Proxy y gratuito pueden ser utilizados en la habilitación de esta interceptación, como se especifica en una sección posterior.

El agente local debe examinar la dirección IP de destino de todos los datagramas que llegan, para ver si es igual a la dirección local de cualquiera de sus nodos móviles registrados fuera de casa. Si es así, el agente local envía por túnel el datagrama hacia la o las direcciones temporales registradas actualmente del nodo móvil. Si el agente local soporta la capacidad opcional de vínculos de movilidad simultáneos múltiples, este envía por túnel una copia a cada dirección temporal en la lista de vínculos de movilidad del nodo móvil. Si el nodo móvil no tiene vínculos de movilidad actuales, el agente local NO debe intentar interceptar datagramas destinados para el nodo móvil, y así no recibirá en general, tales datagramas. Sin embargo, si el agente local es también un router manipulando trafico IP común, es posible que el reciba tales datagramas para pasarlos dentro de la red. En este caso, el agente local debe asumir que el nodo móvil está en casa y simplemente pasa el datagrama directamente dentro de la red local.

Para agentes locales con “múltiples casas” (Multihomed), la dirección de origen en el encabezado IP externo del datagrama encapsulado, debe ser la dirección enviada al nodo móvil en el campo de agente local de la respuesta de registro. Esto es, el agente local no puede usar la dirección de alguna otra interfase de red como la dirección de origen.

Respecto a los métodos de encapsulamiento que pueden ser usados para envío por túneles, hay una sección completa descrita antes al principio de este capítulo, la sección 5.1. Los nodos que implementan túneles deberían también implementar mecanismos “tunnel soft state”, el cual permite a los mensajes de error ICMP regresados desde el túnel, ser reflejados correctamente hacia atrás a los remitentes originales de los datagramas enviados por túneles.

Los agentes locales deben desencapsular los paquetes direccionados a ellos mismos, enviados por un nodo móvil con el propósito de mantener la privacidad de lugar, como se describe en la sección 6.5 del siguiente capítulo; esta característica es también requerida para soportar envío por túneles en reversa.

Si el tiempo de vida para un vínculo de movilidad dado expira antes que el agente local haya recibido otra solicitud de registro válida para ese nodo móvil, entonces ese vínculo es borrado de la lista de vínculos de movilidad. El agente local NO debe enviar ningún mensaje de respuesta de registro simplemente

porque el vínculo de movilidad del nodo móvil ha caducado. La entrada en la lista de visitantes del agente externo actual del nodo móvil expirará naturalmente, probablemente al mismo tiempo que el vínculo expiró en el agente local. Cuando un tiempo de vida del vínculo de movilidad expira, el agente local debe borrar el vínculo, pero debe retener cualquier otro vínculo de movilidad simultáneo (que no haya expirado) que él mantenga para el nodo móvil.

Cuando un agente local recibe un datagrama, interceptado para uno de sus nodos móviles registrados fuera de casa, el agente local debe examinar el datagrama para revisar si este ya está encapsulado. Si es así, se aplican reglas especiales en el reenvío de ese datagrama hacia el nodo móvil:

- Si la dirección de destino interna (encapsulada) es la misma que la dirección de destino externa (el nodo móvil), entonces el agente local debe también examinar la dirección de origen externa del datagrama encapsulado (la dirección de origen del túnel). Si esta dirección de origen externa es la misma que la dirección temporal actual del nodo móvil, el agente local debe descartar silenciosamente ese datagrama, con el objetivo de evitar un posible bucle de enrutamiento. Si, en vez, la dirección de origen externa NO es la misma que la dirección temporal actual del nodo móvil, entonces el agente local debería pasar el datagrama hacia el nodo móvil. Para de pasar el datagrama en este caso, el agente local puede simplemente cambiar la dirección de destino externa a la dirección temporal, en lugar de re-encapsular el datagrama.
- Por el contrario (la dirección de destino interna NO es la misma que la dirección de destino externa), el agente local debería encapsular el datagrama de nuevo (encapsulamiento anidado), con la nueva dirección de destino externa colocada igual a la dirección temporal del nodo móvil. Esto es, el agente local pasa el datagrama entero hacia el nodo móvil de la misma manera como cualquier otro datagrama (ya encapsulado o no).

5.3 DATAGRAMAS BROADCAST

Cuando un agente local recibe un datagrama broadcast, él NO debe pasar el datagrama a ningún nodo móvil en su lista de vínculos de movilidad fuera de aquellos que han solicitado el paso de datagramas broadcast. Un nodo móvil puede solicitar el paso hacia delante de datagramas broadcast, por medio de la configuración del bit “B” en su mensaje de solicitud de registro. Para cada uno de tales nodos registrados, el agente local debería pasar los datagramas broadcast recibidos hacia el nodo móvil, aunque es un problema de configuración en el agente local como para el que serán pasadas categorías específicas de datagramas broadcast a aquellos nodos móviles.

Si el bit “D” fue colocado en el mensaje de solicitud de registro del nodo móvil, indicando que el nodo móvil está usando una dirección temporal co-located, el agente local simplemente envía por túnel datagramas IP broadcast apropiados hacia la dirección temporal del nodo móvil. De lo contrario, (el bit “D” no fue colocado), el agente local primero encapsula el datagrama broadcast en un datagrama unicast dirigido hacia la dirección local del nodo móvil. Este nivel extra de encapsulamiento es requerido de modo que el agente externo pueda determinar cual nodo debería recibir el datagrama, después de que es desencapsulado. Cuando es recibido por el agente externo, el datagrama unicast encapsulado es sacado del túnel y entregado al nodo móvil de la misma forma como cualquier otro datagrama. En cualquier caso, el nodo móvil debe desencapsular el datagrama que recibe, con el objeto de recuperar el datagrama broadcast original.

5.4 ENRUTAMIENTO DE DATAGRAMAS MULTICAST

Como se mencionó previamente, un nodo móvil está conectado a sus funciones de red local de la misma manera que cualquier otro host o router (fijo). Así, cuando él está en casa, un nodo móvil funciona idéntico a otros remitentes y destinatarios multicast. Esta sección por lo tanto describe el comportamiento de un nodo móvil que está visitando una red externa.

Con el objeto de recibir multicast, un nodo móvil debe unir el grupo multicast en una de dos maneras. Primero, un nodo móvil puede unir el grupo vía un router multicast (local) sobre la subred visitada. Esta opción supone que hay un router multicast presente sobre la subred visitada. Si el nodo móvil esta usando una dirección temporal co-located, él debería usar esta dirección como la dirección IP de origen de sus mensajes IGMP. De otro modo, puede usar su dirección local.

De manera alternativa, un nodo móvil el cual desea recibir multicasts puede unir grupos vía túnel bidireccional hacia su agente local, suponiendo que su agente local es un router multicast. El nodo móvil envía por túnel, mensajes IGMP hacia su agente local y el agente local pasa datagramas multicast por el túnel hacia el nodo móvil. Para paquetes enviados por túnel hacia el agente local, la dirección de origen en el encabezado IP debería ser la dirección local del nodo móvil.

Las reglas para la entrega de datagramas multicast hacia nodos móviles en este caso son idénticas a aquellas para datagramas broadcast. A saber, si el

nodo móvil está usando una dirección temporal co-located (el bit “D” fue puesto en la solicitud de registro), entonces el agente local debería enviar por túnel el datagrama hacia esta dirección temporal; de otro modo, el agente local debe primero encapsular el datagrama en un datagrama unicast dirigido a la dirección local del nodo móvil y entonces debe enviar por túnel el datagrama resultante (Tunneling anidado) hacia la dirección temporal del nodo móvil. Por esta razón, el nodo móvil debe ser capaz de desencapsular paquetes enviados hacia su dirección local con el objeto de recibir datagramas multicast usando este método.

Un nodo móvil que desea enviar datagramas hacia un grupo multicast también tiene dos opciones: (1) enviar directamente sobre la red visitada; o (2) enviar mediante un túnel hacia su agente local. Debido a que el enrutamiento multicast en general depende de la dirección IP de origen, un nodo móvil el cual envía datagramas multicast directamente sobre la red visitada debe usar una dirección temporal co-located como la dirección IP de origen. De manera similar, un nodo móvil el cual envía por un túnel un datagrama multicast hacia su agente local debe usar su dirección local como la dirección IP de origen tanto del datagrama multicast (interno) como del datagrama encapsulado (externo). Esta segunda opción supone que el agente local es un router multicast.

5.5 ROUTERS MÓVILES

Un nodo móvil puede ser un router que sea responsable por la movilidad de una o más redes enteras que se mueven juntas, quizá en un avión, un barco, un tren, un auto, una bicicleta o un kayak. Los nodos conectados a una red servidos por el router móvil, pueden ellos mismos ser nodos fijos o nodos móviles o routers. En este documento, tales redes se denominan “redes móviles”.

Un router móvil puede actuar como un agente externo y brindar una dirección temporal de agente externo a nodos móviles conectados a la red móvil. El enrutamiento típico hacia un nodo móvil vía un router móvil en este caso se ilustra por el siguiente ejemplo.

a) Un computador laptop es desconectado de su red local y después unido a un puerto de red en el puesto de atrás de un avión. El laptop usa IP Móvil para registrarse en esta red externa, utilizando una dirección temporal de agente externo descubierta a través de un aviso de agente del agente externo del avión.

b) La red del avión es móvil por si misma. Se puede suponer que el nodo sirviendo como el agente externo sobre el avión también sirve como router por defecto, que conecta la red del avión al resto de Internet. Cuando el avión está en casa, este router está unido a alguna red fija en la oficina principal de la aerolínea, la cual es la red local del router. Mientras el avión está en vuelo, este router registra desde el tiempo que inicia hasta el tiempo que se acaba su enlace de radio con una serie de agentes externos debajo de él en tierra. Este agente local del router es un nodo sobre la red fija en la oficina principal de la aerolínea.

c) Algún nodo correspondiente envía un datagrama al computador portátil, dirigiendo el datagrama a la dirección local del laptop. Este datagrama es inicialmente enrutado a la red local del laptop.

d) El agente local del laptop intercepta el datagrama sobre la red local y lo envía por túnel hacia la dirección temporal del laptop, la cual en este ejemplo, es una dirección del nodo que sirve como router y agente externo sobre el avión. El enrutamiento normal IP enrutará el datagrama hacia la red fija en la oficina principal.

e) El router del avión y el agente local del agente externo allá, interceptan el datagrama y lo envían por túnel hacia su dirección temporal actual, la cual en este ejemplo es algún agente externo sobre tierra debajo del avión. El datagrama original del nodo correspondiente ahora ha sido encapsulado dos veces. Una vez por el agente local del laptop y otra vez por el agente local del avión.

f) El agente externo en tierra desencapsula el datagrama, dando un datagrama todavía encapsulado por el agente local del laptop, con una dirección de destino de la dirección temporal del laptop. El agente externo de tierra envía el datagrama resultante sobre su enlace de radio hacia el avión.

g) El agente externo en el avión desencapsula el datagrama, dando como resultado el datagrama original del nodo correspondiente, con una dirección de destino de la dirección local del laptop. El agente externo del avión entrega el datagrama sobre la red del avión a la dirección de capa de enlace del laptop.

Este ejemplo ilustra el caso en el cual un nodo móvil está unido a una red móvil. Esto es, el nodo móvil es móvil con respecto a la red, la cual es móvil

también por si misma (respecto al suelo). Si, en vez de eso, el nodo es fijo con respecto a la red móvil (la red móvil es la red local del nodo fijo), entonces cualquiera de los dos métodos pueden ser usados para encausar los datagramas desde los nodos correspondientes, para ser enrutados hacia el nodo fijo.

Un agente local puede ser configurado para tener registro permanente para el nodo fijo, que indica la dirección del router móvil como la dirección temporal del host fijo. El agente local del router móvil será usado usualmente para este propósito. El agente local es entonces responsable de avisar conectividad usando protocolos de enrutamiento normales hacia el nodo fijo. Cualquier datagrama enviado hacia el nodo fijo, usará pues, Tunneling anidado como se describió antes.

De forma alternativa, el router móvil puede avisar conectividad a toda la red móvil utilizando protocolos de enrutamiento IP normales, a través de un túnel bidireccional hacia su propio agente local. Este método evita la necesidad de Tunneling anidado de datagramas.

Otros ejemplos de aplicaciones de IP Móvil son las ambulancias que necesitan viajar grandes distancias y que cuentan con una red móvil a bordo, las cuales podrán intercambiar información de diagnóstico y ofrecer tratamiento inmediato a pacientes.

Y por otro lado las Naves guardacostas podrán mantener la conectividad con sus estaciones de tierra mientras patrullan los mares.

5.6 ARP, ARP PROXY Y ARP GRATUITO

“El uso de ARP requiere reglas especiales para la correcta operación cuando nodos inalámbricos o móviles están involucrados. Los requerimientos especificados en esta sección aplican para todas las redes locales en las cuales ARP es usado para resolución de direcciones.

Además del uso normal del ARP para resolución de direcciones de capa de enlace de un nodo determinado, a partir de su dirección IP, en este documento se distinguen dos usos especiales de ARP:

- Un ARP Proxy es una respuesta enviada por un nodo en nombre de otro nodo, el cual es incapaz o está poco dispuesto a responder sus propias solicitudes de ARP. El remitente de un ARP proxy invierte los campos, las direcciones de protocolo de remitente y de objetivo como se describe, pero suministra alguna dirección de capa de enlace configurada (generalmente, la suya) en el campo de dirección de hardware de remitente. El nodo que recibe la respuesta entonces asociará esta dirección de capa de enlace, con la dirección IP del nodo objetivo original, provocándole que transmita futuros datagramas para este nodo objetivo, hacia el nodo con esa dirección de capa de enlace.
- ARP gratuito es un paquete ARP enviado por un nodo, con el objetivo de provocar que otros nodos actualicen espontáneamente una entrada en su cache ARP. Un ARP gratuito puede usar una solicitud de ARP o un paquete de respuesta ARP. En cualquier caso, la dirección de protocolo de remitente ARP y la dirección de protocolo de objetivo ARP, son configuradas con la dirección IP de la entrada cache para ser actualizada, y la dirección de hardware de remitente ARP, es configurada con la dirección de capa de enlace a la cual esta entrada cache debería ser actualizada. Cuando se usa un paquete de respuesta ARP, la dirección de hardware del objetivo es también configurada con la dirección de capa de enlace, a la cual esta entrada cache debería ser configurada (este campo no es utilizado en un paquete de respuesta ARP).

En cualquier caso, para ARP gratuito, el paquete ARP debe ser transmitido como un paquete broadcast local sobre el enlace local. Como se especificó antes, cualquier nodo que recibe algún paquete ARP (solicitud o respuesta) debe actualizar su cache ARP local, con las direcciones de protocolo de remitente y de hardware en el paquete ARP, si el nodo que está recibiendo ya tiene una entrada para esa dirección IP en su cache ARP. Este requerimiento en el protocolo ARP, aplica incluso para paquetes de solicitud ARP y para paquetes de respuesta ARP que no se ajustan a ninguna solicitud transmitida por el nodo receptor.

Mientras un nodo móvil está registrado en una red externa, su agente local usa ARP proxy para responder a las solicitudes ARP que recibe de buscar la dirección de capa de enlace del nodo móvil. Cuando se recibe una solicitud ARP, el agente local debe examinar la dirección IP del objetivo de la solicitud, y si esta dirección IP encaja con la dirección local de cualquier nodo móvil para el cual él tiene un vínculo de movilidad registrado, el agente local debe transmitir una respuesta ARP en nombre del nodo móvil. Después de intercambiar las direcciones de remitente y del objetivo en el paquete, el agente local debe configurar la dirección de capa de enlace del remitente en el paquete, con la dirección de capa de enlace de su propia interfase sobre la cual la respuesta será enviada.

Cuando un nodo móvil abandona su red local y registra un vínculo en una red externa, su agente local utiliza ARP gratuito para actualizar las caches ARP de nodos sobre la red local. Esto provoca que tales nodos asocien la dirección de capa de enlace del agente local con la dirección local (IP) del nodo móvil. Cuando se registra un vínculo para un nodo móvil para el cual el agente local previamente no tenía vínculo (se supuso que el nodo móvil estaba en casa), el agente local debe transmitir un ARP gratuito en nombre del nodo móvil. Este paquete ARP gratuito debe ser transmitido como un paquete broacast sobre el enlace en el cual se encuentra la dirección local del nodo móvil. Desde que los broadcasts sobre el enlace local (tal como Ethernet) no garanticen típicamente ser confiables, el paquete ARP gratuito debería ser retransmitido un pequeño número de veces para incrementar su confiabilidad.

Cuando un nodo móvil regresa hacia su red local, el nodo móvil y su agente local usan ARP gratuito para provocar que todos los nodos sobre la red local del nodo móvil, actualicen sus caches ARP para asociar una vez más, la dirección de capa de enlace propia del nodo móvil, con la dirección local (IP) del nodo móvil. Antes de transmitir el mensaje de solicitud de (des)registro a su agente local, el nodo móvil debe transmitir este ARP gratuito sobre su red local como un broadcast local sobre este enlace. El paquete ARP gratuito debería ser retransmitido un pequeño número de veces para incrementar su confiabilidad, pero estas retransmisiones deberían proceder en paralelo, con la transmisión y el procesamiento de su solicitud de (des)registro.

Cuando el agente local del nodo móvil recibe y acepta esta solicitud de (des)registro, el agente local debe también transmitir un ARP gratuito sobre la red local del nodo móvil. Este ARP gratuito también es utilizado para asociar la dirección local del nodo móvil, con la dirección de capa de enlace propia del nodo móvil. Un ARP gratuito es transmitido tanto por el nodo móvil como por su agente local, siempre y cuando en el caso de interfaces de red inalámbricas, el área dentro del rango de transmisión del nodo móvil probablemente difiera de aquella dentro del rango de su agente local. El paquete ARP desde el agente local, debe ser transmitido como un broadcast local sobre el enlace local del nodo móvil, y debería ser transmitido un pequeño número de veces para incrementar su confiabilidad; estas retransmisiones, sin embargo, deberían proceder en paralelo con la transmisión y procesamiento de su respuesta de (des)registro.

Mientras el nodo móvil está lejos de casa, él NO debe transmitir ninguna solicitud ARP broadcast o mensajes de respuesta ARP. Finalmente, mientras el nodo móvil está lejos de casa, él NO debe responder a solicitudes ARP en las cuales la dirección IP del objetivo sea su propia dirección local, a menos que la solicitud ARP sea unicast por un agente externo con el cual el nodo móvil tiene un registro sin expirar. En el último caso, el nodo móvil debe usar una

respuesta ARP unicast para responder al agente externo. Note que si el nodo móvil está usando una dirección temporal co-located y recibe una solicitud ARP en la cual la dirección IP objetivo es esta dirección temporal, entonces el nodo móvil debería responder a esta solicitud ARP. Note también que, cuando se transmite una solicitud de registro sobre una red externa, un nodo móvil puede descubrir la dirección de capa de enlace de un agente externo, almacenando la dirección como esta es recibida desde el aviso de agente de ese agente externo, pero no transmitiendo un mensaje de solicitud ARP broadcast.

El orden específico en el cual cada uno de los requerimientos anteriores para el uso de ARP, ARP proxy y ARP gratuito son aplicados, relativo a la transmisión y el procesamiento de la solicitud de registro del nodo móvil y los mensajes de respuesta de registro cuando se va de casa o se regresa a casa, es importante para la correcta operación del protocolo. Para resumir los requerimientos anteriores, cuando un nodo móvil deja su red local, se deben ejecutar los siguientes pasos en este orden:

- El nodo móvil decide registrarse lejos de casa, tal vez debido a que ha recibido un aviso de agente de un agente externo y no ha recibido recientemente uno de su agente local.
- Antes de transmitir la solicitud de registro, el nodo móvil inhabilita su propio procesamiento futuro de cualquier solicitud ARP que pueda recibir posteriormente, solicitando la dirección de capa de enlace correspondiente a su dirección local, excepto en la medida que sea necesario para comunicarse con agentes externos sobre redes visitadas.
- El nodo móvil transmite su solicitud de registro.
- Cuando el agente local del nodo móvil recibe y acepta la solicitud de registro, él ejecuta un ARP gratuito en nombre del nodo móvil, y comienza a usar ARP proxy para responder a las solicitudes ARP que recibe solicitando la dirección de capa de enlace del nodo móvil. En el ARP gratuito, la dirección ARP de hardware del remitente es configurada con la dirección de capa de enlace del agente local. Si por el contrario, el agente local rechaza la solicitud de registro, no se ejecuta el procesamiento ARP (gratuito ni proxy) por el agente local.

Cuando un nodo móvil más tarde regresa a su red local, se deben ejecutar los siguientes pasos en este orden:

- El nodo móvil decide registrarse en casa, tal vez porque ha recibido un aviso de agente de su agente local.
- Antes de transmitir la solicitud de registro, el nodo móvil vuelve a habilitar su propio procesamiento futuro de cualquier solicitud ARP que pueda recibir posteriormente, solicitando su dirección de capa de enlace.

- El nodo móvil ejecuta un ARP gratuito para si mismo. En este ARP gratuito, la dirección ARP de hardware del remitente es configurada con la dirección de capa de enlace del nodo móvil.
- El nodo móvil transmite su solicitud de registro.
- Cuando el agente local del nodo móvil recibe y acepta la solicitud de registro, él para de usar ARP proxy para responder a las solicitudes ARP que recibe, solicitando la dirección de capa de enlace del nodo móvil, y entonces ejecuta un ARP gratuito en nombre del nodo móvil. En este ARP gratuito, la dirección ARP de hardware del remitente es configurada con la dirección de capa de enlace del nodo móvil. Si por el contrario, el agente local rechaza la solicitud de registro, el agente local NO debe hacer ningún cambio en la forma como ejecuta el procesamiento ARP (gratuito ni proxy) para el nodo móvil. En este último caso, el agente local debería operar como si el nodo móvil no hubiera regresado a casa, y continuar ejecutando ARP proxy en nombre del nodo móvil."[4]

[4] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

6. CONSIDERACIONES DE SEGURIDAD[5]

El ambiente de informática móvil es potencialmente diferente del ambiente de informática ordinario. En muchos casos, computadores móviles estarán conectados a la red, vía enlaces inalámbricos. Tales enlaces son particularmente vulnerables al espío pasivo del canal, ataques activos de repetición y otros ataques activos.

6.1 CÓDIGOS DE AUTENTICACIÓN DE MENSAJES

Los agentes locales y los nodos móviles deben ser capaces de efectuar autenticación. El algoritmo por defecto es HMAC-MD5, con un tamaño de llave de 128 bits. El agente externo debe también soportar autenticación utilizando HMAC-MD5 y tamaños de llave de 128 bits o más grandes, con distribución de llave manual. Llaves con valores binarios arbitrarios deben ser soportadas.

El uso de “prefijo + sufijo” de MD5 para proteger datos y secretos compartidos es considerado vulnerable para atacar por la comunidad criptográfica. Donde es necesaria compatibilidad hacia atrás con implementaciones de IP Móvil existentes que usan este modo, nuevas implementaciones deberían incluir MD5 en clave, como uno de los algoritmos de autenticación para uso cuando se producen y se verifican los datos de autenticación que son suministrados con los mensajes de registro de IP Móvil, por ejemplo en las extensiones especificadas en las secciones anteriores.

Más algoritmos de autenticación, modos de autenticación métodos de distribución de claves y tamaños de claves pueden también ser soportados para todas y cada una de estas extensiones.

[5] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

6.2 ÁREAS DE SEGURIDAD CONCERNIENTES A ESTE PROTOCOLO

El protocolo de registro descrito a lo largo del trabajo resultará en un tráfico del nodo móvil siendo enviado por túnel hacia su dirección temporal. Esta característica de Tunneling podría ser una vulnerabilidad significativa, si el registro no fue autenticado. Tal redirección remota, por ejemplo la efectuada por el protocolo de registro móvil, es ampliamente entendida como un problema de seguridad en el actual Internet si no es autenticada. Además, el Protocolo de Resolución de Direcciones (ARP) no está autenticado y puede ser utilizado potencialmente para robar otro tráfico de host. El uso de “ARP Gratuito” trae consigo todos los riesgos asociados con el uso de ARP.

6.3 ADMINISTRACIÓN DE CLAVES

Esta especificación requiere un mecanismo de autenticación fuerte (MD5 en clave) el cual excluye muchos ataques potenciales basados en el protocolo de registro IP Móvil. Sin embargo, debido a que la distribución de claves es difícil en ausencia de un protocolo de gestión de claves de red, los mensajes con el agente externo no son requeridos totalmente para ser autenticados. En un ambiente comercial, puede ser importante autenticar todos los mensajes entre el agente externo y el agente local, de tal forma que la facturación sea posible, y los proveedores de servicio no den servicio a usuarios que no son clientes legítimos de ese proveedor de servicio.

6.4 ESCOGIENDO BUENOS NÚMEROS ALEATORIOS

La fortaleza de cualquier mecanismo de autenticación depende de varios factores, incluyendo la fuerza innata del algoritmo de autenticación, la capacidad de mantener en secreto la clave usada, la fuerza de la clave usada y la calidad de la implementación particular. Esta especificación requiere implementación de MD5 en clave para autenticación, pero no excluye el uso de otros algoritmos y modos de autenticación. Para que la autenticación MD5 en clave sea útil, la clave de 128 bits debe ser secreta (esto es, conocida solamente por los grupos autorizados) y pseudo – aleatoria. Si se usan nonces en la conexión con protección de repeticiones, estos deben ser seleccionados con mucho cuidado.

6.5 PRIVACIDAD

Los usuarios que poseen datos sensibles que ellos no quieren que otros los vean deberían usar mecanismos no descritos aquí (tal como encripción) para brindar protección adecuada. Usuarios preocupados por el análisis de tráfico deberían considerar el uso apropiado de encripción de enlace. Si se desea privacidad absoluta de lugar, el nodo móvil puede crear un túnel hacia su agente local. Entonces, los datagramas destinados para nodos correspondientes aparecerán para que provengan de la red local, y puede ser más difícil señalar el lugar del nodo móvil. Aquellos mecanismos están fuera del objetivo de este trabajo.

6.6 FILTRADO DE INGRESO

Muchos routers implementan políticas de seguridad como “filtrado de ingreso”, que no permiten el paso hacia delante de paquetes que tienen una dirección de origen, la cual aparece topológicamente incorrecta. En ambientes donde esto es un problema, los nodos móviles pueden usar envío de paquetes por túnel en reversa con la dirección temporal suministrada del agente externo, como la dirección de origen. Los paquetes enviados por túnel en reversa serán capaces de pasar normalmente a través de tales routers, mientras las reglas de filtrado de ingreso serán todavía capaces de localizar la fuente de topología correcta del paquete, de la misma forma que los paquetes provenientes de nodos no móviles.

6.7 PROTECCIÓN DE REPETICIONES PARA SOLICITUDES DE REGISTRO

El campo identificación es utilizado para dejar que el agente local verifique que un mensaje de registro ha sido generado recientemente por el nodo móvil, no repetido por un atacante de algún registro previo. Dos métodos son descritos en esta sección: timestamps (obligatorio) y “nonces” (opcional). Todos los nodos móviles y agentes locales deben implementar protección de repeticiones basada en estampas de tiempo. Estos nodos pueden también implementar protección de repeticiones basada en nonces.

El estilo de la protección de repeticiones en efecto, entre un nodo móvil y su agente local es parte de la asociación de seguridad móvil. Un nodo móvil y su agente local deben estar de acuerdo con el método de protección que será usado. La interpretación del campo de identificación depende del método de protección de repeticiones, como es descrito en secciones posteriores.

En cualquier método que sea usado, los 32 bits de bajo orden de la identificación deben ser copiados sin cambiar desde la solicitud de registro a la respuesta. El agente externo usa esos bits (y la dirección local del nodo móvil) para ajustar solicitudes de registro con respuestas correspondientes. El nodo móvil debe verificar que los 32 bits de bajo orden de la respuesta de registro son idénticos a los bits que envió en la solicitud de registro.

La identificación en una nueva solicitud de registro NO debe ser la misma que en una solicitud inmediatamente precedente, y NO debería repetirse mientras el mismo contexto de seguridad esté siendo usado entre el nodo móvil y el agente local. La retransmisión es permitida como fue descrita en alguna sección al inicio.

6.7.1 Protección de Repeticiones Usando Estampas de Tiempo. El principio básico de la protección de repeticiones de estampas de tiempo es que el nodo que genera un mensaje inserta la hora del día actual, y el nodo receptor del mensaje revisa que esta estampa de tiempo está suficientemente cerca de su propia hora del día. A menos que se especifique de manera diferente en la asociación de seguridad entre nodos, un valor por defecto de 7 segundos puede ser usado para limitar la diferencia de tiempo. Este valor debería ser mayor que 3 segundos. Obviamente los dos nodos deben haber sincronizado relojes de Hora del día. Como con cualquier mensaje, los mensajes de sincronización pueden estar protegidos contra alteraciones, por un mecanismo de autenticación determinado por el contexto de seguridad entre los dos nodos.

Si se usan estampas de tiempo, el nodo móvil debe configurar el campo de identificación con un valor de 64 bits, formado como se especifica por el Protocolo de Tiempo de Red (NTP). Los 32 bits de bajo orden del formato del NTP representan segundos fraccionales, y aquellos bits los cuales no están disponibles desde una fuente deberían ser generados a partir de una buena fuente de aleatoriedad. Note, sin embargo, que cuando se usan estampas de tiempo, la identificación de 64 bits usada en una solicitud de registro desde un nodo móvil, debe ser mayor que la usada en cualquier solicitud de registro previa, como el agente local usa este campo también como un número de secuencia. Sin tal número de secuencia, sería posible que un duplicado retrasado de una solicitud de registro anterior llegara al agente local (dentro de la sincronización de reloj requerida por el agente local), y así ser aplicada fuera de orden, alterando de manera errónea, la dirección temporal registrada actualmente del nodo móvil.

En el recibo de una solicitud de registro con una extensión de habilitación de autorización, el agente local debe revisar el campo de identificación para validación. Con el objetivo de que sea válido, la estampa de tiempo contenida en el campo de identificación, debe estar suficientemente cerca al tiempo del reloj del día del agente local y la estampa de tiempo debe ser más grande que todas las estampas de tiempo previamente aceptadas para el nodo móvil solicitado. Las tolerancias de tiempo y los detalles de re–sincronización son específicos para una asociación de seguridad de movilidad.

Si la estampa de tiempo es válida, el agente local copia el campo de identificación entero en la respuesta de registro y regresa la respuesta al nodo móvil. Si la estampa de tiempo no es válida, el agente local copia solo los 32 bits de bajo orden en la respuesta de registro, y suministra los 32 bits de orden superior de su propio tiempo del día. En este último caso, el agente local debe rechazar el registro regresando el código 133 (identificación no apropiada) en la respuesta de registro.

El nodo móvil debe verificar que los 32 bits de bajo orden de la identificación en la respuesta de registro, son idénticos a aquellos en el intento de registro rechazado, antes de usar los bits de orden superior para re – sincronización de reloj, tal como se describió antes.

6.7.2 Protección de Repeticiones Usando Nonces. El principio básico de la protección de repeticiones nonce, es que el nodo A incluye un nuevo número aleatorio en todo mensaje hacia el nodo B, y revisa que el nodo B regrese el mismo número en su siguiente mensaje al nodo A. Ambos mensajes usan código de autenticación para proteger contra alteraciones por un atacante. Al mismo tiempo el nodo B puede enviar sus propios nonces en todos los mensajes hacia el nodo A (para ser repetido por el nodo A), de tal forma que este pueda también verificar que él está recibiendo mensajes recientes.

Puede esperarse que el agente local tenga recursos para computar números pseudo –aleatorios útiles como nonces. Él inserta un nuevo nonce como los 32 bits de orden superior del campo de identificación de toda respuesta de registro. El agente local copia los 32 bits de bajo orden de la identificación del mensaje de solicitud de registro, en los 32 bits de bajo orden de la identificación en la respuesta de registro. Cuando el nodo móvil recibe una respuesta de registro autenticada del agente local, él guarda los 32 bits de orden superior de la identificación, para usarlos como los 32 bits de orden superior de su siguiente solicitud de registro.

El nodo móvil es responsable por generar los 32 bits de bajo orden de la identificación en cada solicitud de registro. Idealmente debería generar sus

propios nonces aleatorios. Sin embargo puede usar cualquier método conveniente, incluyendo duplicación del valor aleatorio enviado por el agente local. El método escogido es de preocupación solo del nodo móvil, porque este es el nodo que revisa valores válidos en la respuesta de registro. Los 32 bits de orden superior y de bajo orden de la identificación escogidos deberían diferir ambos de sus valores previos. El agente local usa un nuevo valor se orden superior y el nodo móvil usa un nuevo valor de bajo orden (y la dirección local del host móvil) para ajustar correctamente respuestas de registro con solicitudes pendientes.

Si un mensaje de registro es rechazado debido a un nonce inválido, la respuesta siempre provee al nodo móvil con un nuevo nonce para ser usado en el siguiente registro. Así el protocolo de nonce es auto – sincronizado.[6]

[6] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

7. CONSIDERACIONES DE IANA[7]

IP Móvil especifica varios nuevos espacios de número para valores, para ser usados en varios campos de mensaje. Estos espacios de número incluyen lo siguiente:

- Tipos de mensaje IP Móvil enviados al puerto UDP 434, definido en una sección anterior.
- Tipos de extensiones para mensajes de solicitud de registro y de respuesta de registro.
- Valores para el código en el mensaje de respuesta de registro.
- IP Móvil define los tan nombrados mensajes de solicitud de agente y de aviso de agente. Estos mensajes son de hecho mensajes de descubrimiento de router aumentado con extensiones específicas IP Móvil. De esta manera, ellos no definen un nuevo espacio de nombre, pero definen extensiones de descubrimiento de router adicionales, como se describe más adelante.

Hay espacios de numeración de IP Móvil adicionales especificados.

En la especificación revisada, un nuevo valor de código (para el campo en el mensaje de respuesta de registro) es necesario dentro del rango típicamente usado, para mensajes de agente externo. Este código de error es necesario para indicar el estado “dirección de agente local inválida”.

7.1 TIPOS DE MENSAJE IP MÓVIL

Los tipos de mensajes IP están definidos para ser aquellos que son enviados a un receptor de mensajes en el puerto 434 (UDP o TCP). El espacio de número para mensajes IP Móvil es especificado en las secciones iniciales. La aprobación de nuevos números de extensión es tema de Revisión de Expertos, y se requiere una especificación. Los tipos de mensajes estandarizados actualmente tienen los siguientes números, y son especificados en las

[7] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

secciones correspondientes mucho más atrás pero son los que se especifican en la Tabla 1:

Tabla 1. Tipos de mensajes estándar de IP Móvil

Tipo	Nombre
1	Solicitud de registro
2	Respuesta de registro

Autor.

7.2 EXTENSIONES AL RFC1256 SOBRE AVISO DE ROUTER

El RFC 1256 define dos tipos de mensajes ICMP, Aviso de Router y Solicitud de Router. IP Móvil define un espacio de número para extensiones al Aviso de Router, el cual puede ser usado por protocolos diferentes a IP Móvil. Los tipos de extensión estandarizados actualmente para usar con IP Móvil, tienen los valores de números en el campo Tipo, como se muestra en la Tabla 2 y los cuales se especificaron en el capítulo 3, en los numerales 3.1.1, 3.1.2 y 3.1.3.

Tabla 2. Tipos de extensiones estándar de IP Móvil

Tipo	Nombre
0	Relleno de un bit
16	Aviso de Agente de Movilidad
19	Longitudes prefijas

Autor.

La aprobación de nuevos números de extensión para usar con IP Móvil es tema de Revisión de Expertos, y se requiere una especificación.

7.3 EXTENSIONES A LOS MENSAJES DE REGISTRO DE IP MÓVIL

Los mensajes IP Móvil, especificados en este trabajo, y descritos a lo largo de los capítulos 3 y 4, pueden tener extensiones. Las extensiones de mensaje IP Móvil comparten todas el mismo espacio de número, incluso si ellas están para que sean aplicadas a diferentes mensajes de IP Móvil. El espacio de número para extensiones de mensaje de IP Móvil es especificado a continuación, en la Tabla 3. La aprobación de nuevos números de extensiones es tema de Revisión de Expertos, y se requiere especificación.

Tabla 3. Espacio para extensiones de mensaje IP Móvil

Tipo	Nombre
0	Relleno de un bit
32	Autenticación Móvil – local
33	Autenticación Móvil – Externa
34	Autenticación Externa – Local

Autor.

7.4 VALORES DE CÓDIGO PARA MENSAJES DE RESPUESTA DE REGISTRO DE IP MÓVIL

El mensaje de respuesta de registro de IP Móvil especificado en la sección 4.4, tiene un campo de Código. El espacio de número para los valores del campo Código también es especificado en el mismo numeral del capítulo 4 . El espacio de número es estructurado de acuerdo a que, si el registro fue exitoso, o si el agente externo denegó la solicitud de registro, o en últimas si el agente local denegó la solicitud de registro así:

0-8	Códigos de éxito
9-63	No existen actualmente lineamientos de tarea
64-127	Códigos de error desde el agente externo
128-192	Códigos de error desde el agente local
193-255	No existen actualmente lineamientos de tarea

La aprobación de nuevos valores de Código requiere la Revisión por parte de de Expertos.[8]

[8] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

8. CONSIDERACIONES DE CAPA DE ENLACE[9]

El nodo móvil debe usar mecanismos de capa de enlace para decidir que su punto de conexión ha cambiado. Tales indicaciones incluyen el estado Caído/Probando/Arriba de la interfaz, y los cambios de batería o de administración. Los mecanismos serán específicos para la tecnología de capa de enlace particular, y están fuera del objeto del trabajo.

El Protocolo Punto a Punto (PPP) y su Protocolo de Control del Protocolo de Internet (IPCP), negocian el uso de direcciones IP.

El nodo móvil debería en primer lugar intentar especificar su dirección local, de forma que si el nodo móvil está conectándose a su red local, el enlace sin enrutar funcione correctamente. Cuando la dirección local no es aceptada por el extremo, sino que una dirección IP transitoria es asignada dinámicamente al nodo móvil, y el nodo móvil es capaz de soportar una dirección temporal co-located, el nodo móvil puede registrar esa dirección como una dirección temporal co-located. Cuando el extremo (peer) especifica su propia dirección IP, esa dirección NO debe asumirse como una dirección temporal de agente externo o como la dirección IP de un agente local. Las extensiones PPP para IP Móvil han sido especificadas en el RFC 2290. Si se desean detalles adicionales de cómo manejar asignación de direcciones temporales a partir de PPP de manera más eficiente, por favor consultar el documento mencionado.

[9] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

9. CONSIDERACIONES DE TCP[10]

9.1 TEMPORIZADORES DE TCP

Cuando están en uso enlaces de alto retraso (comunicaciones con satélites) o bajo ancho de banda (radio de alta frecuencia), algunas pilas de TCP pueden tener tiempos fuera de retransmisión insuficientemente adaptativos (no estándar), incluso cuando el enlace y la red están operando adecuadamente, pero solo con un alto retraso debido al medio que se usa. Esto puede causar una inhabilidad para crear o mantener conexiones TCP sobre tales enlaces, y puede también causar retransmisiones innecesarias las cuales consumen el ancho de banda ya escaso. Los vendedores están animados a seguir los algoritmos en el RFC 2988 cuando se estén implementando temporizadores de retransmisión de TCP. Los vendedores de sistemas diseñados para bajo ancho de banda, enlaces de alto retraso, deben consultar los RFC's 2757 y 2488. Los diseñadores de aplicaciones con el objetivo de operar sobre nodos móviles deberían ser sensibles a la posibilidad de dificultades relacionadas con tiempo.

9.2 ADMINISTRACIÓN DE CONGESTIÓN DE TCP

Los nodos móviles a menudo usan medios que son más propensos a introducir errores, causando efectivamente que se pierdan más paquetes. Esto introduce un conflicto con los mecanismos para manejo de congestión encontrados en versiones modernas de TCP. Ahora, cuando un paquete es abandonado, la correspondiente implementación de TCP del nodo, es probable que reaccione como si hubiera una fuente de congestión de red, e inicie los mecanismos de slow-start diseñados para controlar ese problema. Sin embargo, aquellos mecanismos son inadecuados para errores que se superan, introducidos por los enlaces en si, y tienen el efecto de magnificar la discontinuidad introducida por el paquete abandonado. Mientras que las aproximaciones están más allá del alcance de este documento, ellas ilustran que dando transparencia de rendimiento a los nodos móviles, implica entender mecanismos fuera de la capa de red. Los problemas introducidos por tasas de error promedio más altas, también indican la necesidad de evitar diseños los cuales abandonan

[10] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

paquetes sistemáticamente; tales diseños pueden de lo contrario ser considerados favorablemente cuando se hacen ofertas de ingeniería.

10. ESCENARIOS DE EJEMPLO[11]

Esta sección muestra solicitudes de registro de ejemplo para varios escenarios comunes.

10.1 REGISTRO CON UNA DIRECCIÓN TEMPORAL DE AGENTE EXTERNO

El nodo móvil recibe un Aviso de Agente de un agente externo y desea registrarse con ese agente, usando la dirección temporal de agente externo advertida. El nodo móvil desea solamente encapsulamiento IP-en-IP, no quiere broadcasts, y no quiere vínculos de movilidad simultáneos:

- CAMPOS IP
  - Dirección de origen = dirección local del nodo móvil
  - Dirección de destino = copiada de la dirección de origen IP del Aviso de Agente

- Campos UDP
  - Puerto de origen = <cualquiera>
  - Puerto de destino = 434

- CAMPOS DE SOLICITUD DE REGISTRO
  - Tipo = 1
  - S = 0, B = 0, D = 0, M = 0, G = 0
  - Tiempo de vida = el tiempo de vida de registro copiado de la Extensión de Aviso de Agente de Movilidad del mensaje de Aviso de Router
  - Dirección local = la dirección local del nodo móvil
  - Agente local = dirección IP del agente local del nodo móvil
  - Dirección temporal = la dirección temporal copiada de la Extensión de Aviso de Agente de Movilidad del mensaje de Aviso de Router
  - Identificación = estampa de tiempo del Protocolo de Tiempo de Red o Nonce

[11] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

Extensiones: una extensión de habilitación de autorización (por ejemplo la Extensión de Autenticación Móvil – Local)

10.2 REGISTRO CON UNA DIRECCIÓN TEMPORAL CO-LOCATED

El nodo móvil ingresa a una red externa que no contiene agentes externos. El nodo móvil obtiene una dirección a partir del servidor DHCP para usar como una dirección temporal co-located. El nodo móvil soporta todas las formas de encapsulamiento (IP-en IP, encapsulación mínima y GRE), desea una copia de datagramas broadcast en la red local y no desea vínculos de movilidad simultáneos:

- CAMPOS IP
  - Dirección de origen = dirección local del nodo móvil
  - Dirección de destino = dirección IP del agente local
  - Tiempo de vida = 1

- Campos UDP
  - Puerto de origen = <cualquiera>
  - Puerto de destino = 434

- CAMPOS DE SOLICITUD DE REGISTRO:
  - Tipo = 1
  - S = 0, B = 0, D = 0, M = 0, G = 0
  - Tiempo de vida = 0
  - Dirección local = la dirección local del nodo móvil
  - Agente local = dirección IP del agente local del nodo móvil
  - Dirección temporal = la dirección local del nodo móvil
  - Identificación = estampa de tiempo del Protocolo de Tiempo de Red o Nonce

Extensiones: la Extensión de Autenticación Móvil – Local

10.3 ANULACIÓN DE REGISTRO

El nodo móvil regresa a casa y desea desregistrar todas las direcciones temporales con su agente local.

- Campos IP
  - Dirección de origen = dirección temporal obtenida del servidor DHCP
  - Dirección de destino = dirección IP del agente local

- Campos UDP
  - Puerto de origen = <cualquiera>
  - Puerto de destino = 434

- CAMPOS DE SOLICITUD DE REGISTRO:
  - Tipo = 1
  - S = 0, B = 1, D = 1, M = 1, G = 1
  - Tiempo de vida = 1800 (segundos)
  - Dirección local = la dirección local del nodo móvil
  - Agente local = dirección IP del agente local del nodo móvil
  - Dirección temporal = la dirección temporal obtenida del servidor DHCP
  - Identificación = estampa de tiempo del Protocolo de Tiempo de Red o Nonce

Extensiones: una extensión de habilitación de autorización (por ejemplo la Extensión de Autenticación Móvil – Local)

11. APLICABILIDAD DE LA EXTENSIÓN DE LONGITUDES PREFIJAS[12]

La advertencia es indicada con el uso de la extensión de longitudes prefijas sobre enlaces inalámbricos, debido a las áreas de cubrimiento irregulares brindadas por transmisores inalámbricos. Como resultado, es posible que dos agentes externos avisando el mismo prefijo puedan en realidad proveer conectividad diferente a posibles nodos móviles. La Extensión de Longitudes Prefijas NO debería estar incluida en los avisos enviados por agentes en tal configuración.

Agentes externos usando diferentes interfaces inalámbricas, tendrían que cooperar utilizando protocolos especiales para dar igual cubrimiento en el espacio y así ser capaces de reclamar tener interfaces inalámbricas situadas en la misma subred. En el caso de interfaces alámbricas, un nodo móvil que está desconectándose y conectándose posteriormente a un nuevo punto de conexión, puede enviar en una solicitud de registro sin importar si el nuevo aviso está sobre el mismo medio, que el último aviso grabado. Y finalmente, en áreas con poblaciones densas de agentes externos, parecería poco aconsejable requerir la propagación por medio de protocolos de enrutamiento, de los prefijos de subred asociados con cada agente externo inalámbrico individual; tal estrategia podría conducir al agotamiento rápido del espacio disponible para tablas de enrutamiento, incrementos no garantizados en el tiempo requerido para procesar actualizaciones de enrutamiento, y tiempos de decisión más largos para selección de rutas, si las rutas (que son casi siempre innecesarias) son almacenadas para “subredes” inalámbricas.

[12] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

12. CONSIDERACIONES DE INTEROPERABILIDAD[13]

Esta sección especifica revisiones al RFC 2002 que pretenden incrementar la interoperabilidad, mediante la solución de ambigüedades contenidas en el texto anterior. Las implementaciones que ejecutan autenticación de acuerdo con el nuevo algoritmo más precisamente especificado, serían interoperables con implementaciones anteriores que hicieron que se esperara originalmente para producir datos de autenticación. Esa fue la mayor fuente de no-interoperabilidad antes.

Sin embargo, este documento no muestra nuevas facilidades, si se usa, causaría problemas de interoperabilidad con implementaciones antiguas. Todas las características especificadas en el RFC 2002 trabajarán con las nuevas implementaciones, excepto por la compresión V-J o Van Jacobson. La siguiente lista detalla algunas de las posibles áreas de problemas de compatibilidad que pueden ser experimentados por un nodo conforme a esta especificación revisada, cuando intentan interoperar con nodos obedeciendo al RFC 2002.

- Un cliente que espera algunas características obligatorias recientes (como Tunneling en reversa) desde un agente externo estaría inoperable tanto tiempo hasta que preste atención al bit “T”.
- Los nodos móviles que usan la extensión NAI para identificarse a si mismos, no trabajarían con agentes de movilidad antiguos.
- Los nodos móviles que usan una dirección local cero y esperan recibir su dirección local en la respuesta de registro, no trabajarían con agentes de movilidad antiguos.
- Los nodos móviles que intentan autenticarse sin usar la extensión de autenticación Móvil-local, no serán capaces de registrarse exitosamente con su agente local.

En todos estos casos, un nodo móvil robusto bien configurado, es probable que sea capaz de recobrarse si toma acciones razonables en el recibo de una respuesta de registro con un código de error, indicando la causa de este rechazo. Por ejemplo, si un nodo móvil envía una solicitud de registro que es rechazada, debido a que contiene la clase equivocada de extensión de autenticación, entonces el nodo móvil podría volver a intentar el registro con

[13] Texto basado en el documento IP Mobility Support for IPv4 de la IETF. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

una extensión de autenticación móvil-local, siempre y cuando el agente externo y/o agente local en este caso, no esté configurado para demandar los datos de autenticación alternativos.

13. MENSAJES DE EJEMPLO

13.1 EJEMPLO DE FORMATO DE MENSAJE DE AVISO DE AGENTE ICMP

Figura 30. Formato de mensaje de aviso de agente ICMP

0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
TIPO	**CÓDIGO**	**CHECKSUM**
NÚMERO DIRECCIÓN	**TAMAÑO DE ENTRADA DE DIRECCIÓN**	**TIEMPO DE VIDA**
DIRECCIÓN DE ROUTER [1]		
NIVEL DE PREFERENCIA [1]		
DIRECCIÓN DE ROUTER [2]		
NIVEL DE PREFERENCIA [2]		
...		
TIPO = 16	**LONGITUD**	**NÚMERO DE SECUENCIA**
TIEMPO DE VIDA DE REGISTRO	**R B H F M G r T**	**RESERVADO**
DIRECCIÓN TEMPORAL [1]		
DIRECCIÓN TEMPORAL [2]		
...		
EXTENSIONES OPCIONALES ...		

Autor.

13.2 EJEMPLO DE FORMATO DE MENSAJE DE SOLICITUD DE REGISTRO

El encabezado UDP está seguido por los campos IP Móvil que se muestran a continuación:

Figura 31. Formato de mensaje de solicitud de registro

0 1 2 3 4 5 6 7	8 9 0 1 2 3 4 5	6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
TIPO = 1	**S B D M G r T x**	**TIEMPO DE VIDA**
DIRECCIÓN LOCAL		
AGENTE LOCAL		
DIRECCIÓN TEMPORAL		

IDENTIFICACIÓN		
EXTENSIONES DE NO AUTORIZACIÓN OPCIONALES PARA AGENTE LOCAL... (Longitud Variable)		
TIPO = 32	LONGITUD	SPI
SPI (Cont.)		
AUTENTICADOR NODO MÓVIL – AGENTE LOCAL (Longitud Variable)		
EXTENSIONES DE NO AUTORIZACIÓN OPCIONALES PARA AGENTE EXTERNO ... EXTENSIÓN DE AUTENTICACIÓN NODO MÓVIL - AGENTE EXTERNO OPCIONAL ...		

Autor.

13.3 EJEMPLO DE FORMATO DE MENSAJE DE RESPUESTA DE REGISTRO

El encabezado UDP está seguido por los campos IP Móvil que se muestran a continuación:

Figura 32. Formato de mensaje de respuesta de registro

0										1										2										3	
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
TIPO = 3										CÓDIGO										TIEMPO DE VIDA											
DIRECCIÓN LOCAL																															
AGENTE LOCAL																															
IDENTIFICACIÓN																															
EXTENSIONES DE NO AUTORIZACIÓN OPCIONALES DE AGENTE LOCAL... (Longitud Variable)																															
TIPO = 32										LONGITUD										SPI											
SPI (Cont.)																															
AUTENTICADOR NODO MÓVIL – AGENTE LOCAL (Longitud Variable)																															
EXTENSIONES OPCIONALES UTILIZADAS POR AGENTE EXTERNO ... EXTENSIÓN DE AUTENTICACIÓN NODO MÓVIL - AGENTE EXTERNO OPCIONAL ...																															

Autor.

14. VENTAJAS Y DESVENTAJAS DE IP MÓVIL VERSIÓN 4 FRENTE A IP MÓVIL VERSIÓN 6

14.1 VENTAJAS DE MIP6 VS MIP4

- Optimización de rutas
- Coexistencia con filtrado de ingreso
- Las opciones de destino de IPv6 permiten emplear piggybacking en lugar de usar mensajes de señalización adicionales. Esto quiere decir que los reconocimientos de recibo en el destino son enviados “montados” dentro del paquete y no en mensajes o paquetes adicionales.
- Al usar la autoconfiguración de IPv6, no hace falta la presencia de un Agente Externo.
- Los avisos de vecinos que envían los Agentes Locales para interceptar el tráfico hacia un nodo móvil son independientes del nivel físico (ARP no).
- Se puede hacer Descubrimiento Dinámico de Agente Local (Dynamic Home Agent Discovery) usando Anycast, es decir enviando paquetes de solicitud de agente mediante difusión a cualquier destino.

14.2 PROBLEMAS DE IP MÓVIL

- Pérdidas durante el proceso de traspaso: los datagramas que están en el camino hacia el Agente Externo desde el Agente Local cuando se produce un cambio de localización del móvil hacia otro agente externo se pierden (paquetes en vuelo).
- Eficiencia del traspaso: si la red está muy lejos, cada cambio de localización requiere el registro/desregistro del agente local. El traspaso a una red cercana espacialmente requiere actualizarse en un lugar muy alejado, por lo tanto hay una falta de eficiencia.

15. IMPLICACIONES HUMANÍSTICAS

Al ir un poco más allá de la parte netamente tecnológica y científica acerca del Protocolo IP Móvil, y al adentrarse en las profundidades de este, referentes a sus facilidades, beneficios, usos y sobretodo su relación directa con el entorno del ser humano, es posible encontrar que este invento, creación, descubrimiento o como se quiera llamar trae consigo muchos más aspectos favorables que inconvenientes, al igual que la mayoría de innovaciones que han surgido a lo largo de la historia del hombre.

De este modo, tomando como base que la dimensión del hombre abarca muchos temas que van desde la epistemología y la antropología, pasando por la filosofía y la política, hasta llegar a la ética y la sociología, es posible enmarcar la tecnología IP Móvil en cada uno de estos tópicos de acuerdo con su relación y sus implicaciones para la vida de la humanidad.

En primer lugar, como ya se ha mencionado en la introducción y a lo largo del documento, la tecnología IP Móvil solo traerá para el hombre beneficios desde todos los puntos de vista; si uno se mete de lleno en el tema de la epistemología, se pensaría que no tiene nada que ver con esto, sin embargo sucede todo lo contrario. La epistemología es la ciencia que estudia el conocimiento científico y por esta razón está directamente ligada a cualquier descubrimiento que haga el hombre. De esta forma lo único que trae para el hombre la búsqueda y el hecho de encontrar algo nuevo que pueda beneficiarlo, lo hace un ser altamente desarrollado y hace que se diferencie del resto de los seres vivientes que habitan este planeta.

Pero no solo el hombre o persona creadora de conocimiento es quien le saca provecho a sus inventos, sino que los individuos que logran tener acceso a este conocimiento pueden aumentar sus conocimientos, de manera que en un momento determinado puedan transmitir su sabiduría a las generaciones subsiguientes, sin importar el método para hacerlo, pues hoy en día basta con consultar libros, bibliotecas y el mismo Internet, el cual ha sido una de las invenciones más grandes de los últimos años a nivel de tecnologías de comunicaciones y el cual es y ha sido la base para nuevos desarrollos como IP Móvil, gracias a que está basado en el Protocolo IP, fundamento de Internet. Como se puede ver el conocimiento del hombre no se queda estancado, sino que está en continuo proceso de perfeccionamiento.

Con respecto a la dimensión netamente humana, es decir lo que tiene que ver con la relación del hombre, entendido como un grupo de personas, con sus semejantes y las implicaciones que tiene el descubrimiento, desarrollo y aplicación de cualquier cosa novedosa, se puede decir que el hombre se ha caracterizado siempre por ser un ser social, el cual requiere interactuar con los que lo rodean, quienes pueden ser muy importantes para cierta persona, en este caso su familia, sus amigos y hasta sus compañeros de trabajo. Por tal motivo, es importante para la humanidad buscar y encontrar soluciones que le permitan tener una mejor calidad de vida desde todos los puntos de vista, especialmente en lo que tiene que ver con las relaciones interpersonales, lo cual ha sido considerado siempre; por ejemplo, muchas veces se pensó que el teléfono sería un invento solo para minorías y que era muy complicado tenerlo, pero hoy se piensa en que es un medio de acercamiento para las personas que están lejos, o que es una forma de permitir el intercambio de palabras, de información y hasta de sentimientos, lo cual hace que el hombre se sienta muy bien cuando habla por este aparato. Igual sucede con ciertos inventos, que a pesar de que no son tan perceptibles como el teléfono o el televisor, en el fondo hacen de la vida algo mucho más agradable; es el caso de la tecnología IP Móvil.

Gracias a que el Protocolo IP Móvil permite comunicarse en tiempo real, un individuo que en un momento dado necesite información de su empresa, de su familia o de sus amigos, siempre la recibirá a tiempo sin necesidad de estar cerca o en un punto fijo. Esto sucedía antes, pues una persona que siempre estaba conectado a una red de comunicaciones nunca podía recibir mensajes o información si no estaba allí conectado, lo cual hace que se sienta impotente, incomunicado, solo y hasta en casos extremos, abandonado. Por otra parte, IP Móvil brinda un sentimiento de tranquilidad a quien lo utilice, pues a pesar de que no es algo fácil de explicar, si un sujeto sabe que cuenta con él cuando está lejos de su sitio habitual, se sentirá seguro, útil e importante para las personas que lo requieren, mejorando su autoestima y sus relaciones sociales con el resto del mundo que cada vez está más globalizado.

El milagro de las comunicaciones, que cada día son más y más avanzadas, afectan de manera relevante no solo la parte social y de conocimiento del hombre sino también las dimensiones política y económica del mundo entero. Es muy bien sabido que la finalidad de un invento es el beneficio en primer lugar de la persona que lo hace o lo descubre, gracias a su interés por solucionar un problema, sin embargo cuando una tecnología se pone al alcance de todo el mundo, los beneficios son mucho mayores, ya que afectan no solo la parte de motivación de las personas, sino que a gran escala puede afectar el desarrollo de una nación entera, impulsando el trabajo, el comercio, la investigación, etc. En resumen, una innovación afecta el aspecto político-económico de un grupo de personas, bien sea un grupo pequeño como el familiar, u otras agrupaciones mayores como un barrio, un pueblo, una ciudad o un país.

IP Móvil hará de este mundo, un mundo cada vez más integrado, más comunicado y más desarrollado, pues puede promover los negocios de manera mucho más dinámica, el intercambio de información entre dirigentes del gobierno, y en sí el desarrollo de la economía en otras formas hasta ahora, nunca antes vistas. Por ejemplo, debido a que al Protocolo IP Móvil está relacionado estrechamente con el Protocolo IP, base de Internet, puede lograrse una mayor integración de las redes de comunicaciones de todo el mundo para permitir el desarrollo exponencial de muchas aplicaciones, generando una cultura de confianza y aceptación poco a poco.

Desde el punto de vista ético, cabe decir que todas las implicaciones que pueda tener un descubrimiento dependen única y exclusivamente del pensamiento y del uso que le pueda llegar a dar un individuo, pues se entiende que lo que se busca es el bien y no el mal, pero como ya ha sucedido con muchos inventos y descubrimientos como la pólvora, los celulares, el ADN, y otros, se les han encontrado nuevas utilidades que no son precisamente ejemplares para el mundo, y es posible que se lleguen a determinar usos indebidos para las nuevas tecnologías de las comunicaciones, como ya está ocurriendo actualmente.

Se puede pensar que esta tecnología puede llegar a reemplazar el protocolo IP del todo, pero básicamente depende de muchos factores, como el grado de aceptación de la humanidad, el grado de uso, desarrollo, las implicaciones económicas y demás aspectos que solo pueden ser estudiados una vez la tecnología sea algo real y aceptada de forma masiva. Por ahora solo se puede afirmar que el grado de beneficio o problema que pueda llegar a tener, depende exclusivamente del hombre.

16. INFORME DE PASANTÍA

Como requisito de la práctica de la carrera de Ingeniería de Telecomunicaciones, y como solicitud del jurado encargado de revisar el presente trabajo, se ha establecido informar mediante una sección separada acerca de los trabajos y actividades adelantadas o desarrolladas durante el período de trabajo de grado en la modalidad de pasantía. Por esta razón el objeto de este pequeño informe es dar a conocer todas y cada una de las actividades llevadas a cabo en la empresa SIEMENS S.A. alrededor de los seis (6) meses de práctica. Cabe anotar que la presente descripción está basada en un informe previo que fue presentado al ingeniero Jorge Humberto Muñoz al cabo de haber transcurrido tres (3) meses de pasantía.

En primer lugar es necesario mencionar que el trabajo desarrollado en la empresa Siemens dependen del área en la que se trabaje y que no todas las tareas que se realizan en Siemens son labores netamente técnicas, ni tampoco muy enfocadas al área de ingeniería donde se hacen diseño de soluciones o al área de servicios donde se hacen actividades de configuración, instalación y montaje de equipos y soluciones complejas; en mi caso, por el contrario las actividades que yo desarrollé fueron netamente administrativas enfocadas por supuesto a lo técnico y otras tareas de apoyo en lo que se pudiera y llegara a necesitar.

Durante el periodo que perduró la pasantía estuve trabajando en un área tiene un jefe, el cual está a cargo de otras seis (6) personas cada una de ellas encargada a desarrollar un negocio, enfocado por ejemplo a servicios, otro a equipos y así sucesivamente cada uno de ellos muy bien distinguido, incluyendo una nueva área que hasta ahora está empezando, que se trata de todo lo referente al tema de Seguridad.

Al cabo de estos meses, mi labor se centró en colaborarles a todos ellos en la recepción, análisis, desarrollo, integración y feliz término o entrega de licitaciones, para participar en los negocios del área de informática y comunicaciones que surgen cada día. Sin embargo esta tarea no sólo abarca las diferentes licitaciones públicas que se presentan, sino que también cubre ofertas voluntarias e invitaciones para concursar, tanto a nivel nacional como internacional, ya que por ser una empresa multinacional, la característica más notable es que los negocios se pueden dar a nivel de la Región Andina (Colombia, Venezuela, Perú y Ecuador), Sudamérica y Centroamérica, entre otros lugares.

Entre los proyectos en los cuales tuve la oportunidad de trabajar se encuentran, licitaciones grandes, proyectos referentes a la prestación de servicios, lo cual esta en su auge y también y trabajé en otras que tratan la instalación de equipos y soluciones, junto con sus respectivos servicios. Todo lo relacionado con estas propuestas y ofertas tuvo que ver con la parte administrativa pero siempre guardando una relación estrecha con las soluciones técnicas.

De manera un poco más particular, se puede decir que en estos meses me dediqué a hacer presentaciones con los datos y aspectos más importantes de un proyecto a desarrollar, así como también, realicé lecturas y entendimiento de los diferentes pliegos de condiciones para poder visualizar el alcance de los proyectos, todo ello acompañado de listas de documentos y listas de requerimientos y hasta algunas condiciones comerciales.

Entrando en detalles, algunas de las tareas que desarrollé y que son netamente administrativas, como ya lo había mencionado, fueron la búsqueda de información en Internet para nuevas oportunidades de negocios, búsqueda de información en la Intranet para uso interno y externo, búsqueda de posibles partners para la elaboración de un proyecto, traducciones de documentos inglés-español y español-inglés, e incluso de portugués a español para entregar a los clientes y para actividades estratégicas, elaboración de presentaciones para mostrar el alcance de los proyectos, elaboración de tablas de precios y cotizaciones, descriptivos de las soluciones entregadas a los clientes, respuestas a pliegos e integración de las propuestas para entregar en los días y horas señaladas.

También tuve la oportunidad de participar en algunas de las actividades que se llevan a cabo dentro del curso normal de los procesos de contratación o licitaciones, como visitas obligatorias, audiencias de aclaraciones y de cierre de los procesos, junto con sus adendas y reuniones internas para decidir responsables en los proyectos.

Como puede notarse, el trabajo no es muy técnico, pero se aprenden muchas cosas respecto al manejo de una empresa y del negocio como tal, aplicando conceptos vistos a lo largo de la carrera de Ingeniería de Telecomunicaciones, y de materias como economía, gestión de proyectos, entre otras. Pude aprender sobre algunas tecnologías propias de Siemens, así como de algunas que no lo son; aprendí a trabajar bajo presión hasta altas horas de la noche y hasta los fines de semana, pues me tocó colaborar en algunos proyectos que requieren mucha más dedicación y tiempo, que otros de menor envergadura.

Respecto a mi trabajo de profundización, es decir este documento, puedo decir que lo realicé con un ritmo constante y fue avanzando, poco a poco, durante los seis (6) meses de práctica.

Finalmente, pienso que faltó un poco involucrarme más en la parte de cotizaciones y manejo de costos y precios, lo cual es lo más importante y lo que más me gusta actualmente, pero que a la vez es lo más demorado en conseguir pues se debe entender que no se pueden dar tantas responsabilidades a unos “simples” practicantes que hasta ahora están comenzando.

Solo resta por decir que tenía muchas expectativas con respecto a quedarme trabajando allí en Siemens, y poder conocer otra área diferente y así poder experimentar más y adquirir mayor conocimiento. Afortunadamente lo logré, gracias al esfuerzo y al empeño que puse en dos proyectos desarrollados en el último mes de la pasantía.

17. CONCLUSIONES

Se ha podido mostrar la tecnología IP Móvil como un protocolo muy importante para nuevos desarrollos y facilidades en el área de las comunicaciones, por su estrecha relación con el protocolo IP, el cual es la base de los actuales sistemas de información a nivel mundial. La descripción del protocolo como el método de comunicación entre dos puntos, la forma en su estructura interna, es decir sus campos, su capacidad de llevar información y de dirigirla correctamente han sido descritos con bastante profundidad y de una manera tan completa que permite a cualquier persona entender claramente el funcionamiento de esta tecnología, para nuevas aplicaciones en los sistemas de comunicaciones en el mundo.

El poderlo dar a conocer de alguna manera a todas las personas como una de las nuevas tecnologías puede llegar a ser la solución para la migración de redes privadas a públicas, basados en el protocolo IP, hace de este documento algo que puede llegar a ser de mucha utilidad y de mucha ayuda para el aprendizaje de los estudiantes de la Universidad Santo Tomás e Ingenieros de Telecomunicaciones o afines que no tienen conocimiento del protocolo IP Móvil y sus características y facilidades.

En la práctica, a través del análisis del trabajo se puede ver la trascendencia que puede llegar a tener el protocolo IP Móvil en el sector de las telecomunicaciones, de varias maneras, pues esta tecnología no solo está enfocada a brindar movilidad, flexibilidad y comodidad a los usuarios de empresas del sector, sino que también puede servir como respuesta a los problemas de comunicación y de acceso a las redes, para pequeñas, medianas y grandes empresas que utilizan las tecnologías de la información, entre las cuales se encuentran las empresas del sector de la educación, del gobierno y la industria.

IP Móvil permitiría mayores facilidades como la comunicación en tiempo real sin pérdida de tiempo ni de información, mayor interconectividad a nivel mundial, mayor control sobre la información recibida desde otros puntos remotos, seguridad, desenvolvimiento sencillo, flexibilidad y sobretodo el concepto de movilidad, el cual es la característica que está surgiendo como la tendencia actual y también como un estándar futuro.

La nueva tecnología IP Móvil, una vez implementada, hará la vida del hombre mucho más sencilla y confortable, pues lo único que traerá consigo será tranquilidad, estabilidad en su grupo familiar, social y laboral mediante un

desarrollo personal y social más completo, para realizar sus labores diarias con el resto del mundo de una manera eficiente y dinámica, sin depender su sitio de trabajo (estático).La persona que utilice IP Móvil se sentirá parte integral de una organización a pesar de estar fuera de ella, pues nunca perderá contacto con ella, ni con otras organizaciones que en determinado momento deseen comunicarse.

IP Móvil es y/o se perfila como un beneficio a nivel mundial, pues al observar los ejemplos tan claros y tan sencillos de entender, descritos a lo largo del trabajo, se visualiza su utilidad tanto en redes corporativas fijas, como en redes móviles, redes pequeñas, medianas y grandes, y en general en toda la Red Extensa Mundial IP "www" más conocida como Internet.

BIBLIOGRAFÍA

Apuntes tomados durante las clases de Telemática I y II en la Universidad Santo Tomás.

Documento Internet Engineering Task Force: Request For Comments RFC 2002 “IP Mobility Support”.

Documento Internet Engineering Task Force: Request For Comments RFC 2003 “IP Encapsulation within IP”.

Documento Internet Engineering Task Force: Request For Comments RFC 2004 “Minimal encapsulation within IP”.

Documento Internet Engineering Task Force: Request For Comments RFC 768 “User Datagram Protocol”.

Documento Internet Engineering Task Force: Request For Comments RFC 791 “Internet Protocol”.

Documento Internet Engineering Task Force: Request For Comments RFC 1256.

WEBGRAFÍA

ARTÍCULO. Howto-Mip. [Documento en Línea]. 2002 Disponible en Internet < www.oasis.dit.upm.es/~cdc/HOWTO-MIP >

ARTÍCULO. Mobile IP. Documento en Línea]. 2002. Disponible en Internet < www.ahciet.net/tecnologia/ redes_infraestructura/telcordia05.pdf >

ARTÍCULO. Mobile IP: una solución para proporcionar la movilidad de los terminales en Internet. [Documento en Línea]. 2004. Disponible en Internet < http://acimut.upf.es/moliver/OlL99.pdf >

DEPARTAMENTO DE INGENIERÍA DE LA INFORMACIÓN Y LAS COMUNICACIONES. Redes Móviles. [Documento en Línea]. 2003/2004. Disponible en Internet < http://ants.dif.um.es/rm/apuntes/Tema3-RM.pdf >

FACULTAD DE CIENCIAS FISICO-MATEMÁTICAS. Resumen de IP Móvil. [Documento en Línea]. 2002. Disponible en Internet < http://mx.geocities.com/AdmonRedes/EquipoTresTema2.htm >

IETF. IP Mobility Support for IPv4. [Documento en Línea]. 11 junio de 2004. Disponible en Internet < http://www.ietf.org/proceedings/04aug/ I-D/draft-ietf-mip4-rfc3344bis-00.txt >

LUCARES SANTIBAÑEZ ALEJANDRO. Comunicaciones móviles. [Documento en Línea]. 2004. Disponible en Internet < http://www.acapomil.cl/investigacion/ boletines/boletin_2004/articulos/moviles.htm >

TRABAJO. IP Móvil. [Documento en Línea]. 2002. Disponible en Internet < http://www.infor.uva.es/~jvegas/docencia/ar/seminarios/IPMovil.pdf >

TRABAJO. IP Móvil. [Documento en Línea]. 2002. Disponible en Internet < http://www.redes.upv.es/~mperez/rc2/trabajos/IPMOVILTxT.pdf >

TUTORIALES. Sistema IP – Móvil. [Documento en Línea]. 2002. Disponible en Internet < http://www.angelfire.com/ri2/grupo1/tutoriales/Sistema_IP.doc >

WINDOWS TI MAGAZINE. Artículo Como instalar y configurar una red Wi-Fi. [Documento en Línea]. 2003. Disponible en Internet < http://www.windowstimag.com/atrasados/2003/73_mar03/articulos/enportada_wifi.asp >