Internet Engineering Task Force
INTERNET DRAFT
draft-itsumo-hmmp-00.txt
Date: October 1999
Expires: April 2000

Faramak Vakil
Ashutosh Dutta
Jyh-Cheng Chen
Telcordia Technologies

Shinichi Baba
Yasuro Shobatake
Toshiba Research America,Inc.

Host Mobility Management Protocol
Extending SIP to 3G-IP Networks
<draft-itsumo-hmmp-00.txt>

Status of this Memo

This document is an Internet-Draft and is in full conformance with all provisions of Section 10 of RFC2026.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts. Internet- Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

To view the list Internet-Draft Shadow Directories, see http://www.ietf.org/shadow.html.

The distribution of this memo is unlimited. It is filed as <draft-itsumo-hmmp-00.txt>, and expires April, 2000. Please send comments to either farm@research.telcordia.com or sbaba@tari.toshiba.com.

Copyright Notice

ABSTRACT

Host mobility management protocol (HMMP) is a protocol for supporting real-time and non-real-time multimedia applications on mobile terminals of 3G-IP networks. HMMP utilizes as well as extends session initiation protocol (SIP) to provide means of domain hand-off (i.e., roaming), and subnet hand-off (i.e., macro mobility) so that users can access the network from any location using their own mobile

terminal. An advantage of HMMP is that it can spoof constant endpoints for mobile TCP connections and supports mobile TCP applications in a SIP environment without any changes to the TCP.

The objective of this document is to present the preliminary specifications of HMMP, identify the impact of mobility on SIP, and propose necessary extensions to ensure that SIP can support roaming users adequately. Specifically, it proposes that

a. the SIP INFO method provides a means of profile verification and/or replication, and address binding, b. the SIP REGISTER method designates a "RHO" CONTACT that allows the registrar to obtain a new address from the DHCP on behalf of the mobile, c. the SIP user agent is equipped with a SIP_EYE agent that maintains a record of ongoing TCP connections of the mobile, and d. the SIP user agent understands address binding INFO messages and takes necessary actions.

Furthermore, it proposes that either the DHCP interact with the DNS and update it dynamically, or a new protocol be developed to allow applications to use SIP registrar for name to address and address to name mappings.

1.Introduction

1.1 The Rationale

Driving the trend towards third generation wireless IP (3G-IP) technology are users' demand for perpetual ubiquitous access to the Internet, rapid proliferation of mobile Internet appliances, and providers' desire for deploying a flexible wireless and wireline IP platform that supports heterogeneous services economically [1, 2, 3]. Furthermore, the current wisdom is that the existing circuit switched and 1G/2G (i.e., 1G and 2G) wireless systems will eventually evolve and merge into an end-to-end IP platform that provides ubiquitous real-time as well as non-real-time services. In a nutshell, it is envisioned that an end-to-end wireless/wireline IP platform comprising 3G wireless access networks and a wireline IP backbone will support real-time and non-real-time multimedia services in the future. Thus, supporting roaming users is an essential feature of the end-to-end signaling and control system of IP networks as well as a critical topic for consideration in the IETF SIP working group.

1.2 3G-IP Requirements and Issues

A 3G-IP network is a wireless platform that will enable mobile users' IP appliances to access multimedia services on end-to-end

wireline/wireless IP platforms in future [6]. We envision that it will

- eventually be built upon the packet mode capabilities of the 3G wireless technologies such as IMT-2000 [4, 5],

- support mobile real-time and non-real-time services such as mobile telephony, mobile web access, and mobile data services [7, 8],

- provide means of global roaming, offer intelligent services (e.g., call forwarding, etc.) similar to those of today's intelligent networks,

- strive to ensure that the quality (and price) of their service offerings will be comparable to those of today's wireless telephony and data services, and

- be built upon enhancements of the current IETF standards to the extent possible so that the design and development cycle is minimized.

Among the key issues in the design of the signaling and control system of 3G-IP networks are how to

+ support terminal as well as personal/user mobility,

+ satisfy the quality of service (QoS) requirements of services, particularly those of real-time applications for roaming users,

+ ensure privacy and security of the users as well as the network resources,

+ perform billing and accounting, and

+ maintain smooth interworking with the public switched telephone network (PSTN) and its 1G/2G wireless access networks.

Although each of these issues may have some impact on the signaling protocols of IP networks that are being developed in the SIP working group, addressing all of them is beyond the scope of this document. This document exclusively focuses on the specifications of a mobility management protocol that uses an extended version of SIP to support multimedia services of roaming users.

1.3 Scope and Purpose

The objective of this document is to present the preliminary specifications of host mobility management protocol (HMMP). We

- build upon the personal mobility feature of SIP to design HMMP that suppots terminal as well as personal mobility,
- identify the impact of mobility on SIP, and
- propose necessary extensions to ensure that SIP can support roaming users via HMMP adequately.

HMMP is a protocol for supporting real-time and non-real-time multimedia applications on mobile terminals. It provides means of domain hand-off (i.e., roaming), and subnet hand-off (i.e., macro mobility). However, HMMP primarily relies on the link layer to support the cell-hand-off (i.e., micro-mobility). HMMP also spoofs constant endpoints for mobile TCP connections and supports mobile TCP applications in a SIP environment without any changes to the TCP.

1.4 Related IETF Documents

HMMP is primarily built upon the session initiation protocol (SIP) as specified in RFC 2543. Other related IETF documents are
- SDP: Session Description Protocol (RFC 2327),
- DHCP: Dynamic Host configuration Protocol (RFC 2131),
- IP Encapsulation within IP (RFC 2003), and
- Minimal Encapsulation within IP (RFC2004).

1.5 Organization of the Document

This document is organized as follows. HMMP's assumptions on the underlying network environment are summarized in Section 2, where Section 2.1 describes the architecture of a 3G-IP network, and Section 2.2 summarizes its signaling architecture that is the substrate of HMMP. Section 3 provides an overview of the HMMP operation and underscores the need for augmenting the SIP user agent with a SIP_EYE agent that tacks ongoing TCP connections of the mobile station. Section 4 contains the detailed specifications of HMMP where we describe how HMMP utilizes SIP to provide means of registration, location service, and hand-off to roaming users. The function and basic operation of the SIP_EYE agent are described in Section 5. In Section 6, we summarize the impact of supporting mobility via HMMP on SIP specifications, and highlight necessary extensions for supporting mobility with SIP. Finally, Section 7 concludes the document with open issues for further study.

2. Assumptions: A 3G-IP Environment

This Section provides an overview of a 3G-IP network and its signaling architecture that serves as the foundation of HMMP.

2.1 Architecture of a 3G-IP Network

Figure 1 depicts the end-to-end packet platform of a 3G-IP network, which comprises 3G-IP access networks and a packet switched IP backbone network. The IP backbone network is an end-to-end wireline IP infrastructure that will comprise regional providers' wireline IP networks that are connected through the Internet. Besides mobile stations/terminals, a wireless access network usually comprises a set of base stations, base station controllers, and mobile switching centers [3]. In order to support the needs of its users, a wireless access network interacts with the network control and signaling entities that are shown as "Signaling & MAAAQ" in Figure 1. What follows is a brief description of these elements and their functions.

Mobile Station (MS)

It is the user mobile terminal that allows users to communicate, and also provides means of interaction (i.e., signaling) between users and the network.

Base Station (BS)

It is an adaptive remote radio multiplexer/demultiplexer that provides physical and link layer functions and essentially serves as a MAC layer repeater. In IMT-2000 programmable software radios can be used to provide flexibility across frequency bands at the MS and the BS.

Base Station Controller (BSC)

It is a multi-port bridge (or switch) with an IP interface to MSC that interacts with the network control and management system (via the MSC) to control and manage base stations. A BSC may control one or more BSs.

Mobile Switching Center (MSC)

An MSC is an IP router that connects the wireless access network and the regional wireline IP network. In the IP parlance, each MSC is the default gateway of all IP MSs that are supported by BSCs that are connected to it. A couple of points are worth noting. First, different BSCs may be connected to different ports of an MSC. Second, the BSC and MSC functions may be implemented either in a single physical entity, or as two separate entities.

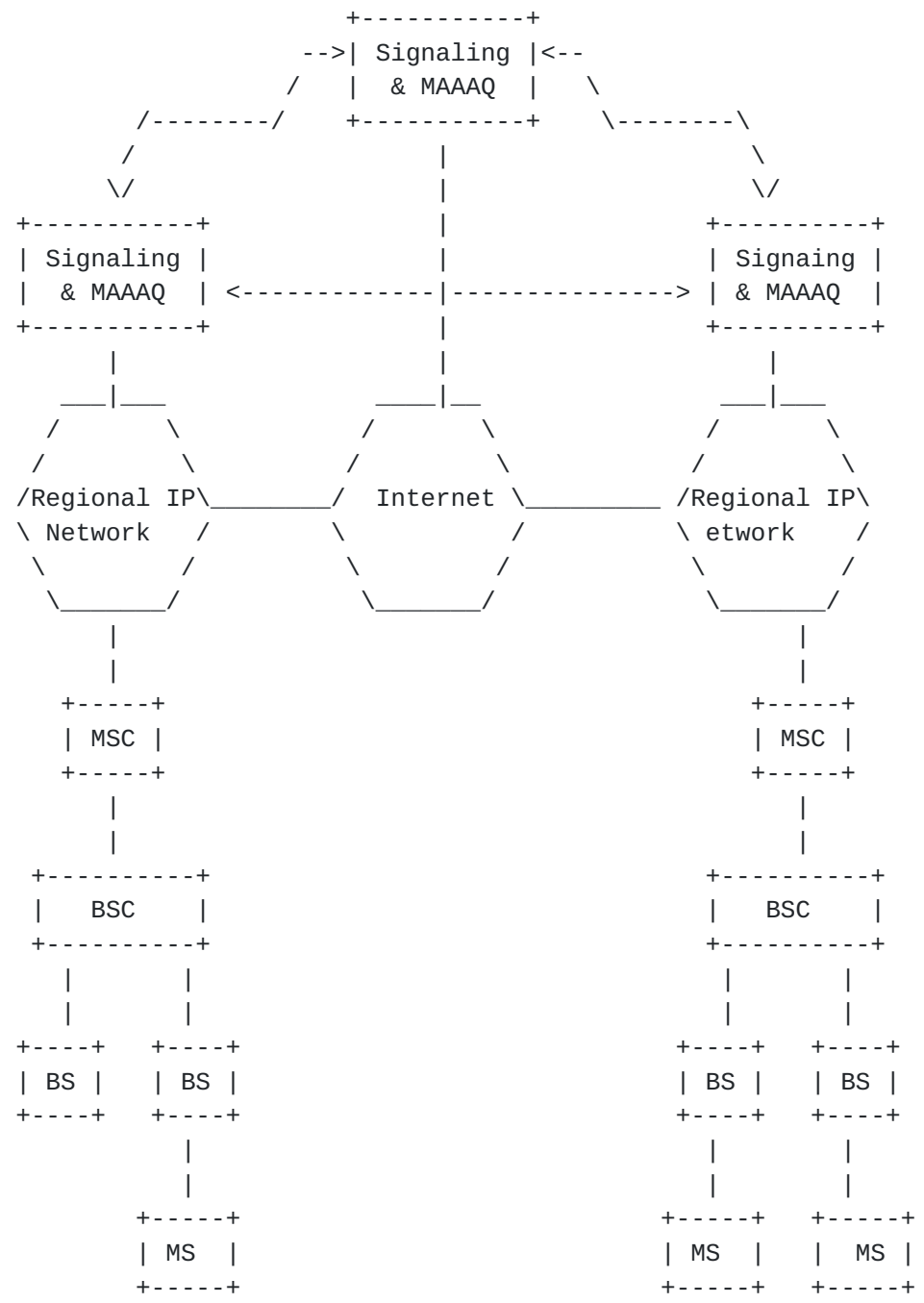


Figure 1. End-to-end network architecture of a 3G-IP network

Signaling & MAAAQ

Signaling provides connection management as well as means of interaction between users and network control system and interaction among network control entities. MAAAQ (Mobility, Authentication, Authorization, Accounting, and QoS) entities support mobility management, AAA, and QoS management functions for mobile users. These

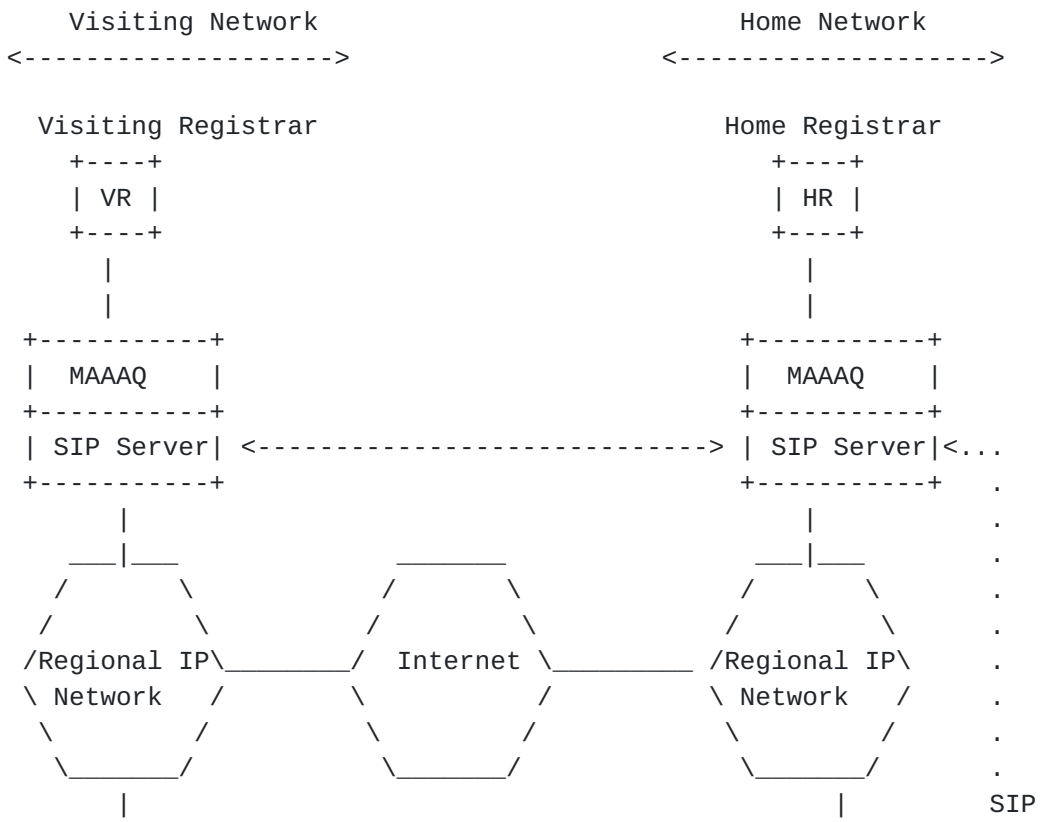
functional entities usually reside on the wireline backbone, and are

part of the overall signaling and control system of the end-to-end platform. As Figure 1 indicates the home and visiting signaling & MAAAQ entities may either interact directly or via a third party signaling & MAAAQ entity on the global Internet. In the latter case, the third party signaling & MAAAQ entity serves as a trusted broker between the home and visiting network signaling and MAAAQ entities.

2.2 A Signaling Architecture for 3G-IP Networks

The overall signaling architecture of a 3G-IP is shown in Figure 2. It uses session initiation protocol (SIP) [9, 10] as the basis of its end-to-end signaling and control architecture. The rationales for the choice of SIP are that:

- SIP is a lightweight end-to-end protocol with a small set of messages that can be used for user as well as network node signaling.
- SIP uses a single request message for session initiation, and scales well over wide-area networks.
- SIP is ideal for IP mobiles, enables mobiles to perform some intelligent networking functions themselves, and supports non-IP mobiles via a customer gateway.
- SIP provides a means of personal mobility that is a crucial part of mobility management in wireless environments.



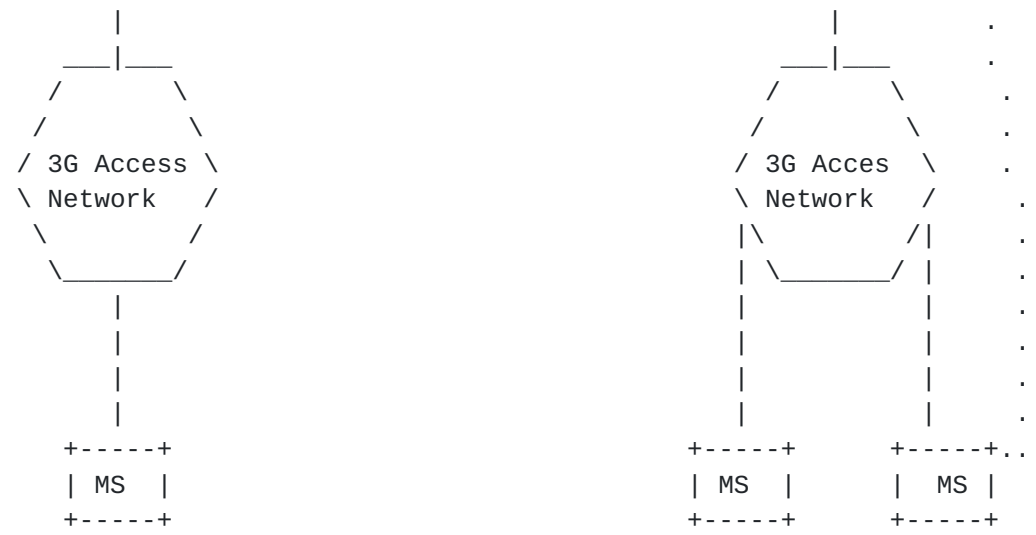


Figure 2. A signaling architecture for 3G-IP networks

All MSs and fixed hosts have SIP user agents that provide means of interactions with the SIP servers (i.e., proxy servers, redirect servers, and registrar) within the network. In Figure 2, the SIP server entity of a regional IP network represents the set of SIP proxy and SIP redirect servers within the regional network that perform the network control and signaling functions. Similarly, the registrar represents the server (or set of servers) that accepts (accept) SIP REGISTER requests and provides (provide) location services that are similar to those of the home/visiting location registries (HLR/VLR) in today's wireless telephony. As Figure 2 shows the MAAAQ entity is built on top of SIP, and uses the location and signaling services of SIP to support roaming users.

The illustration of the MAAAQ entities and SIP server as a single module in Figure 2 shall not be interpreted as a requirement for having a centralized SIP server or MAAAQ entity per regional network. Figure 2 only shows the required functions, though each of the SIP and MAAAQ entities comprise a set of distributed agents. Similarly, the SIP registrars (i.e., HR and VR) may be implemented as either central or distributed databases.

The remainder of this document focuses primarily on the specifications of a HMMP for the mobility management entity as well as necessary extensions to SIP for supporting roaming users.

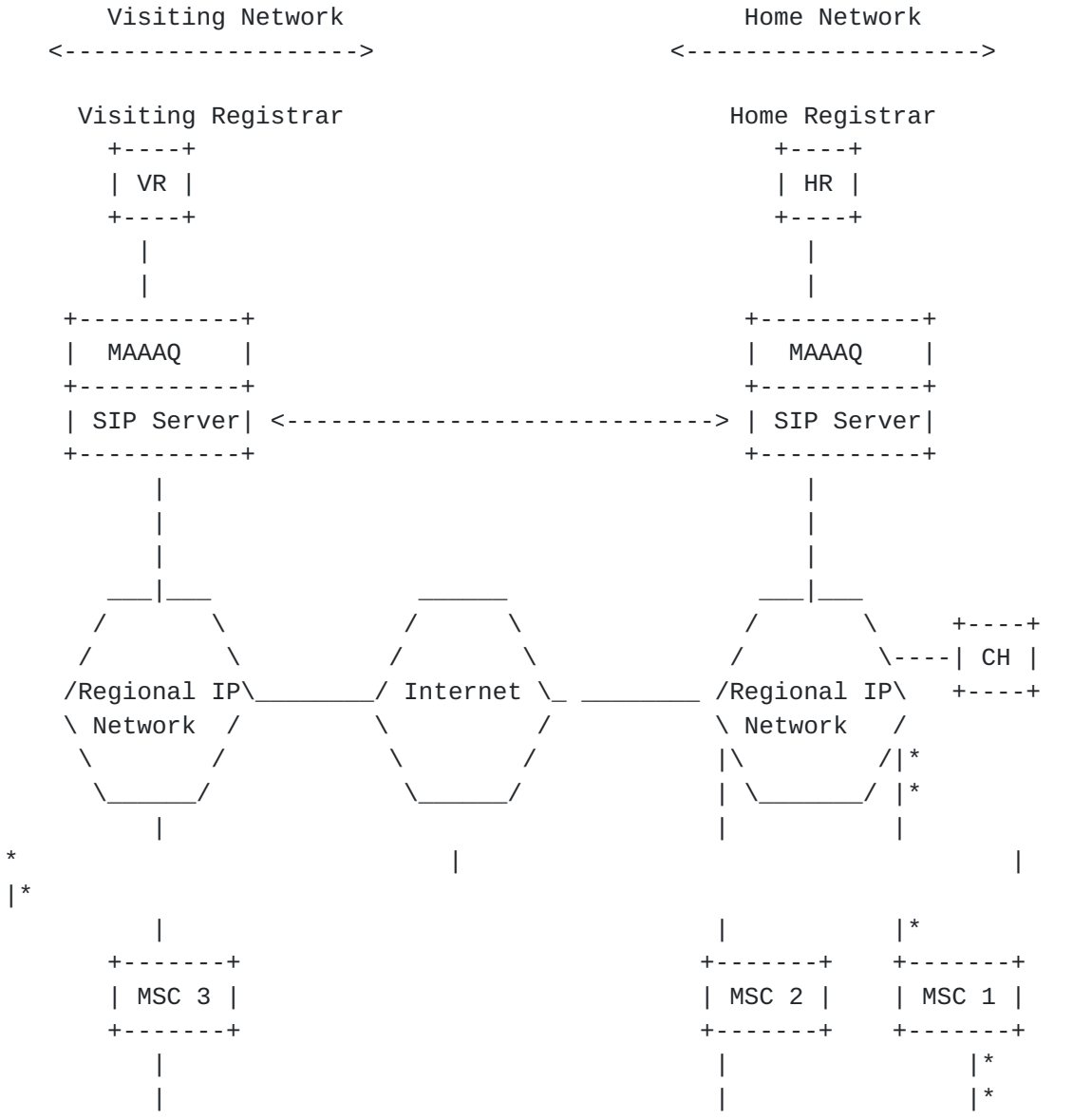
3. An Overview of HMMP

Figure 3 depicts an end-to-end 3G-IP platform in relative detail. Let us consider the scenario where a corresponding host communicates with a mobile host. For the sake of discussion, let us assume that

- the mobile has already registered with its home network using SIP REGISTER method, and
- its communication with the corresponding host starts when it is at point A and continues as it moves towards point D.

In general, a mobility management protocol shall provide three functions to the mobile users. These functions are

i. cell hand-off (micro mobility): that allows users to move from a cell to another, i.e., moving between base stations from A to B,
ii. subnet hand-off (macro mobility): that allows users to move between different subnets within the same administrative domain from B to C, and
iii. roaming (global mobility): that allows users to roam between different subnets that belong to different administrative domains from C to D.




+----------+
| BSC 3 |
+-------+
| BSC 2 |
+----------+
| BSC 1 |

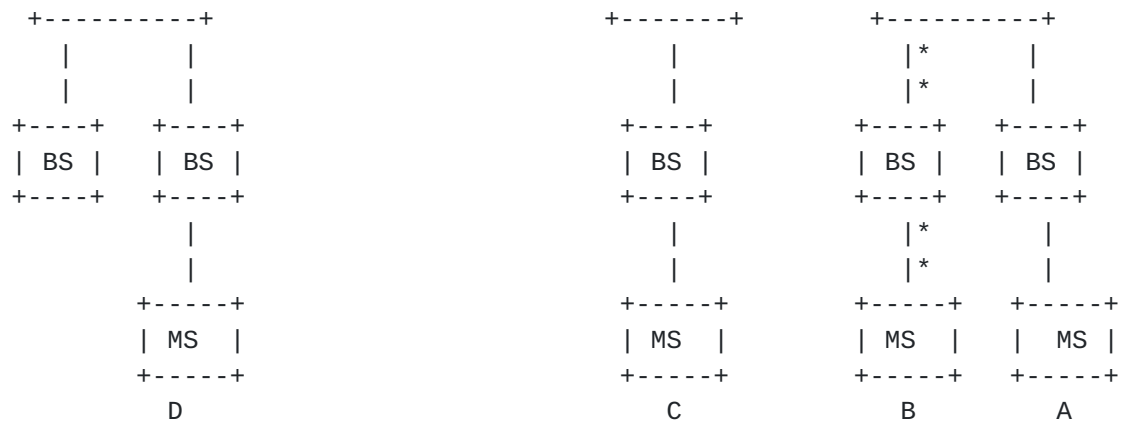


Figure 3. Cell hand-off in HMMP

The cell hand-off (i.e., micro mobility) is not part of HMMP and is usually handled at the link layer, while HMMP uses SIP to provide the subnet hand-off (i.e., macro mobility) and roaming (i.e., global mobility) functions for mobile hosts on 3G-IP networks. What follows is a walk through the operation of HMMP using this example.

3.1 Cell hand-off

As the mobile moves from A to B, then the link layer mobility management entity

* binds the mobile's MAC address (or CDMA sequence) to the BSC port destined for base station B, and
* updates the label translation table in BSC 1, so that the information destined for the mobile host is routed to base station B. Note that the label translation table refers to a table in the BSC that contains the binding of mobile's MAC addresses to BSC ports.

If the mobile can communicate with two adjacent base stations simultaneously, the mobile's binding to base station A may be maintained for a time-out period after the hand-off so that the hand-off is soft and transient packets are not lost. Note that the IP address of the mobile remains the same.

3.2 Subnet hand-off

The mobile moves further from B to C, and it is still registered with the network. HMMP supports subnet hand-off (i.e., macro mobility) during the session as follows.

+ The mobile asks a new temporary address from DHCP. The mobile

requests a new address either directly (see Section 4.1.1) or via a SIP registrar (see Section 4.1.2). The DHCP gives the mobile a temporary IP address, the address of its default gateway, and the subnet mask. Furthermore, the DHCP updates the domain name system (DNS) simultaneously.

+ In public networks, the network authenticates the mobile as a protection against fraud. In principle, it is always desirable to authenticate a mobile before assigning network resources such as adresses to it. For instance, PPP has its own registration scheme using CHAP during session initiation and the MIP extension using NAI for registration prpose has been proposed. The registration approach described in Section 4.1.2 as well as the Dynamic Registration and Configuration Protocol(DRCP) proposed in McAuley, et.al [14] both can authenticate and assign an address to it simultaneously.
+ The mobile or SIP server re-invites the corresponding host to the temporary address (similar to the approach proposed by Wedlund and Schulzrinne [16]).
+ SIP server and network resource reservation scheme should create a new route with adequate resources between the corresponding host and the mobile.
  a. This new route with adequate resources is only created for real-time applications like voice. There have been several proposal for the use of Resource ReServation Protocol (RSVP)[21] for resource reservation in wireline networks that have SIP signaling [22]. However, due to its receiver initiated reservation scheme, RSVP is not suitable for a mobile wireless netwok. The specifications of a resource reservation mechanism for supporting real-time mobile applications and its interaction with SIP require further study, and are beyond the scope of this document.
  b. The non-real-time applications are allowed to traverse the network hop-by-hop.
+ The mobile or SIP server ensures that the transient data is forwarded to the new address, i.e., it creates a short-lived tunnel between MSC 1 and MSC 2 to reduce loss of the transient data due to hand-off. In order to create this tunnel, the mobile or SIP server informs MSC-1 to bind the previous address of the mobile to its current one for a time-out period. This requires
  * SIP user agents at all MSCs (i.e., subnet routers), and
  * the address of the most recent MSC which is the most recent default gateway.

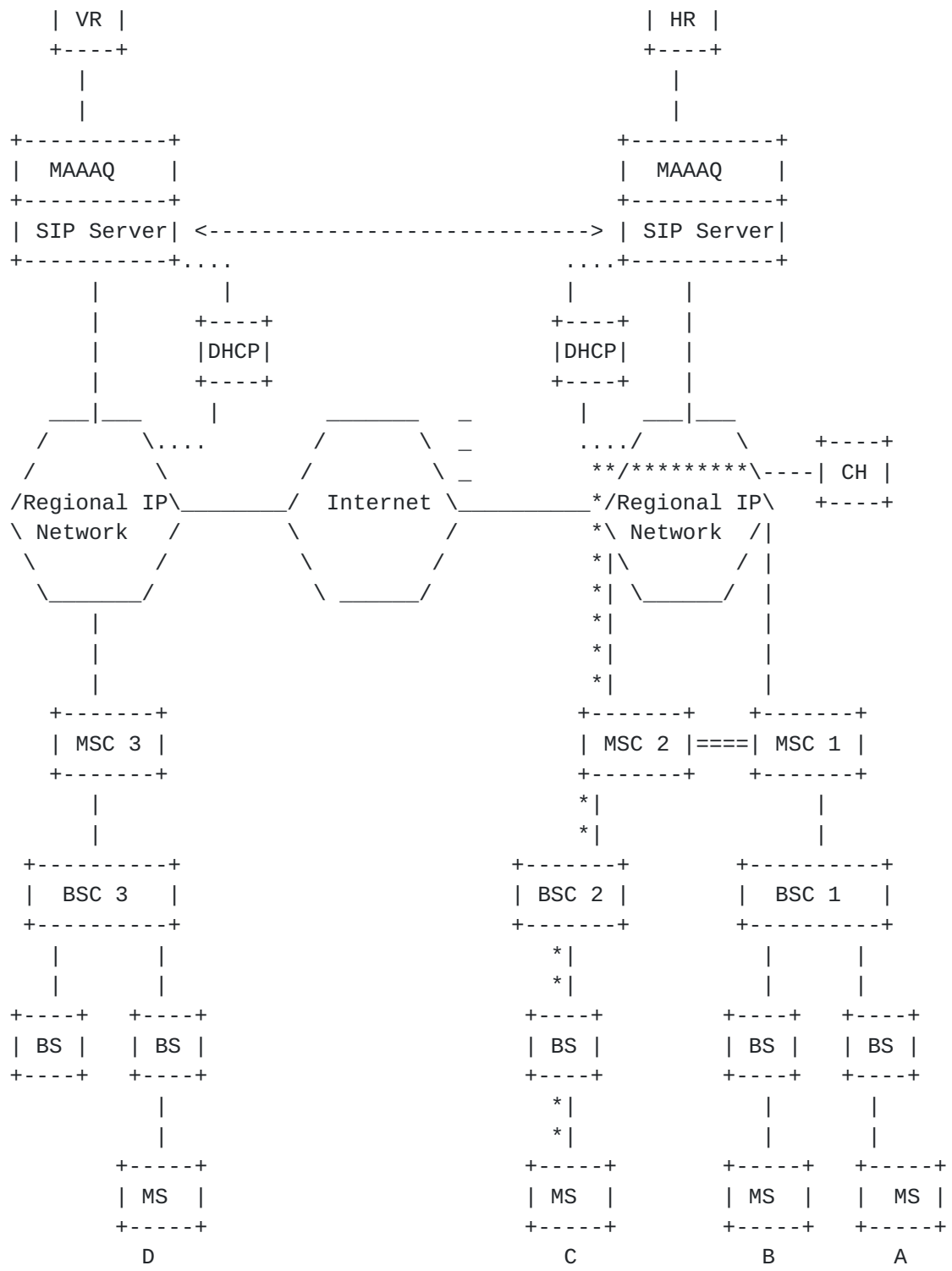


Figure 4. Subnet hand-off in HMMP

3.3 Roaming

Except for the fact that the mobile SHALL always be autheticated, roaming in HMMP is similar to subnet hand-off described in Section 3.2. As the mobile moves further to D, HMMP operates as follows:

+ The mobile requests for a temporary address and receives one from DHCP. The DHCP updates the DNS simultaneously.
+ The mobile re-registers with its temporary address in the new domain using the SIP REGISTER method.
    * The mobile profile is added to the visiting registrar (VR), i.e., its profile is replicated either through interaction of the VR with the HR or by pre-planned profile replications [13] in the neighboring VRs. The pre-planned profile replications reflect the mobility pattern of the mobile, and its effective realization requires continuous monitoring of users' mobility patterns.
+ The mobile or SIP server re-invites the corresponding host to the temporary address (similar to the approach proposed by Wedlund and Schulzrinne [16]).
+ SIP server and network resource reservation scheme should create a new route with adequate resources between the corresponding host and the mobile.
  a. This new route with adequate resources is only created for real-time applications like voice. The specifications of a resource reservation mechanism for supporting real-time mobile applications and its interaction with SIP require further study, and are beyond the scope of this document.
  b. The non-real-time applications are allowed to traverse the network hop-by-hop.
+ The mobile or SIP server ensures that the transient data is forwarded to the new address, i.e., it creates a short-lived tunnel between MSC 2 and MSC 3 to reduce loss of the transient information
+ The mobile or SIP server informs MSC-2 to bind the previous address of the mobile to its current one for a time-out period. This requires
  * SIP user agents at all MSCs (i.e., subnet routers), and
  * the address of the most recent MSC which is the most recent default gateway.

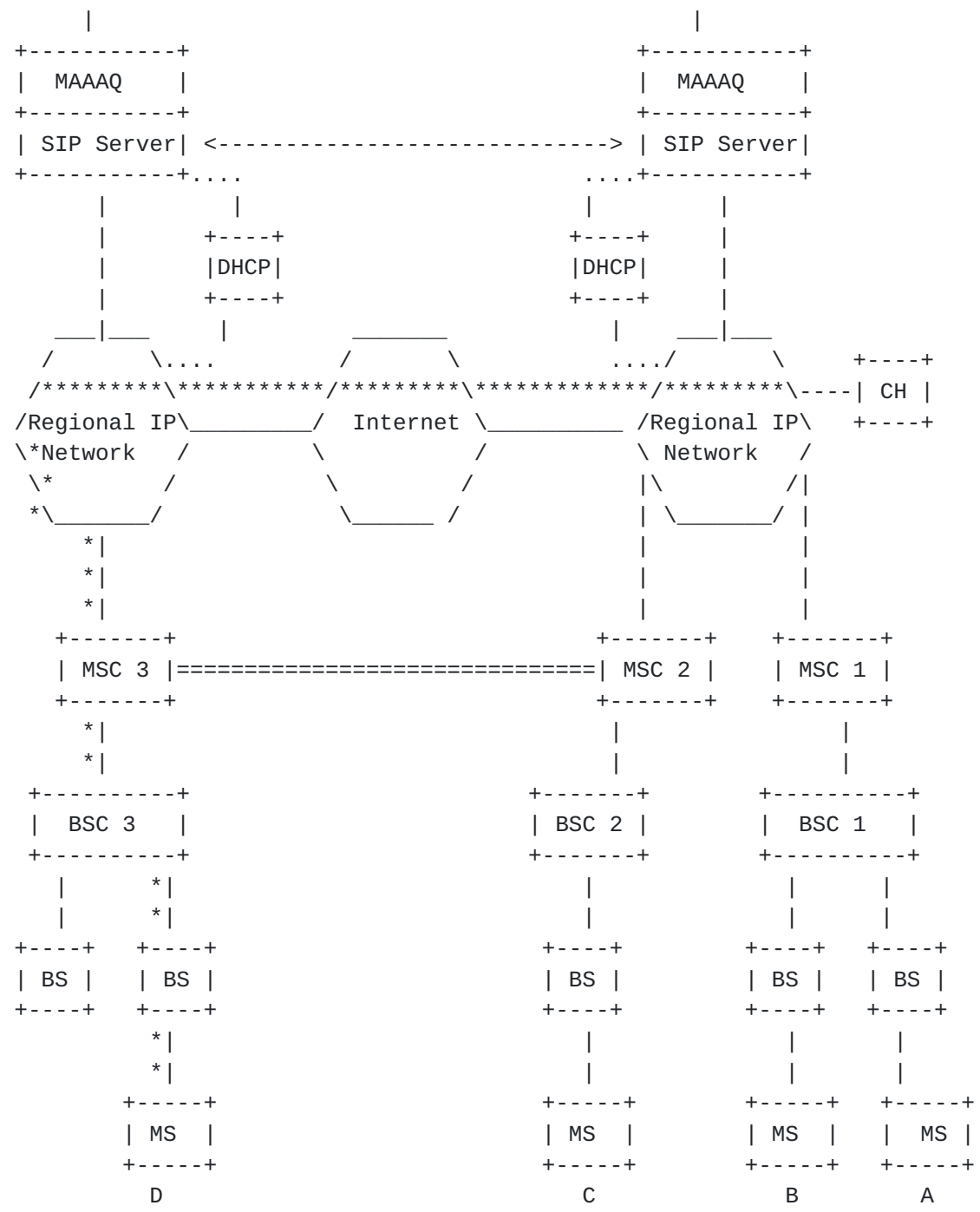


Figure 5. Roaming in HMMP

3.4 Supporting TCP Applications with HMMP

Internet applications that require a reliable service from the transport mechanism, e.g., file transfer protocol (FTP), primarily use TCP. Thus, it is essential that HMMP support mobile TCP

applications without requiring any changes to the TCP.

Although the fundamental abstraction of both SIP and TCP is the connection, they identify it differently. A session/call ID identifies a SIP connection/session, while a pair of endpoints identifies a TCP connection. Each TCP endpoint is identified with a pair of integers (host, port) where host is IP address of the endpoint, and port is the TCP port on the host. However, as a mobile roams, its IP address, i.e., the host integer of its TCP endpoint changes. In order to support TCP applications properly, HMMP shall spoof constant TCP endpoints despite changes in their host integers (i.e., IP addresses) due to roaming of the mobiles. The spoofing process is akin to mobile IP with route optimization [17, 18], and its underlying idea is that

- the mobile informs the corresponding TCP endpoints about its new address,
- the corresponding host(s) binds (bind) the initial IP address of the mobile with its new temporary (i.e., care of address) IP address, and
- the corresponding host(s) uses (use) encapsulation to send the TCP packets bearing the initial source and destination addresses to the current location/address of the mobile.

In order to support TCP applications on HMMP without modifying TCP, the SIP user agent SHALL be augmented with a SIP_EYE agent that tracks TCP connection set-ups and releases within the mobile. The SIP_EYE agent enables the SIP user agent to maintain a record of mobile's ongoing TCP connections, and their identifiers. SIP_EYE operates as follows:

i. It examines headers of TCP packets to monitor the birth and death of TCP connections as well as identify their endpoints, i.e., the source and destination IP addresses and port numbers of these connections.
ii. It maintains a current record of the mobile's ongoing TCP connections' identifiers, and the address of the current and last (i.e., most recent) MSCs (i.e., default gateways) within the mobile's SIP user agent.
iii. SIP_EYE records a state comprising four integers, <original MS IP address, previous MS IP address, current MS IP address, original corresponding IP address>, per TCP connection. The original MS IP address is the IP address of the mobile at the beginning of the TCP session, previous mobile IP address is the last IP address of the mobile just before its current one, and current MS IP address is the current IP address of the mobile. The original corresponding IP address is the IP address of the corresponding host at the beginning of the

TCP session.

iv. Upon a mobile station's successful registration with the visiting network, its SIP user agent sends
   (a) an INFO message (messages) to the SIP user agent(s) of corresponding host(s) to request binding of the original address of the mobile with its current one, and
   (b) also sends a INFO message to last MSC for binding the previous host address to the new one so that a short-lived tunnel is created for forwarding transient data to the mobile's location.

v. The corresponding host and the MSC use IP encapsulation (either within IP [19] or minimal [20]) to forward the TCP information to the mobile's current location.

The key advantage of this approach is that TCP stays as is; though the required IP encapsulation reduces the bandwidth efficiency of the channel.

Since the DHCP interacts with DNS to dynamically update the name to address and address to name mappings, new TCP connections will be established using the current address of the mobile. Another alternative for name to address mapping and vice-versa is that instead of a dynamic DNS, one develops a new protocol that allows applications to use SIP registrar for name to address and address to name mappings. The specifications of this alternative and its comparison with a dynamic DNS scheme require further study, and is beyond the scope of this docuement.

4. HMMP on SIP

SIP supports personal mobility function. HMMP builds upon the personal mobility feature of SIP to enable users to access the network from any location using their own mobile terminal. The two main functions of HMMP are registration, and mobility support. The registration involves assigning new address to a roaming mobile and authenticating it whenever necessary; while the mobility support comprises re-invitation, and/or tunneling via address binding. Let us explain how one can utilize and extend SIP to perform these functions.

4.1 Registration

SIP REGISTER method allows users to register with the network and enable them to access the network from any terminal on the network. HMMP utilizes SIP to register and configure mobile terminals. There are two ways to use SIP for mobile registration. The first approach requires no extension/modifications of SIP, while the second requires certain modifications and extensions of SIP.

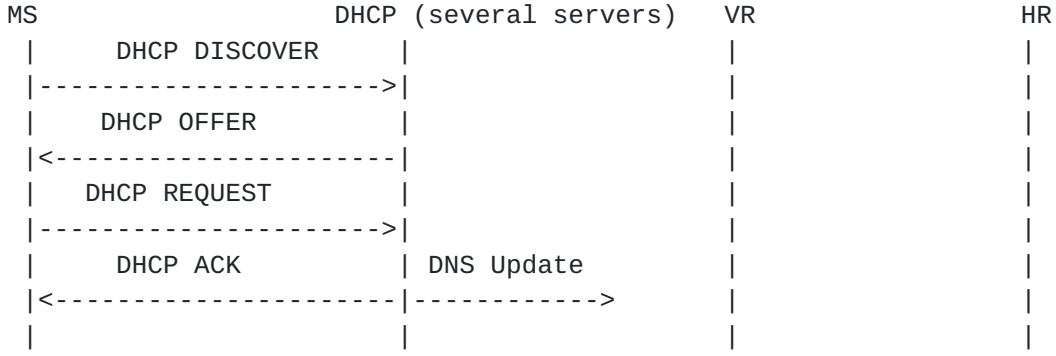
4.1.1 Registration: Approach 1

The first registration approach utilizes the dynamic host configuration protocol (DHCP) [11], and SIP REGISTER and recently proposed INFO method [12] to perform the registration. It operates as follows.

+ The mobile station (MS) requests a new address from DHCP.
+ DHCP assigns a temporary address to the MS.
+ The MS uses SIP REGISTER method with its temporary IP address as CONTACT in the REGISTER method. Note that if this registration is trigrred by the roaming of the MS in the middle of an ongoing session (i.e., re-registration), then the visiting registrar (VR) shall authenticate it with the home registrar (HR).

The signaling flow for the registration is depicted in Figure 6. The MS broadcasts a DHCPDISCOVER message to the DHCP servers. Several servers offer a new address to MS via DHCPOFFER; the MS selects one and sends a DHCPREQUEST to the corresponding DHCP server. The DHCP server send a DHCPACK to confirm the assignment of the address to the MS. Simultaneously, the DHCP SHALL update the DNS address to name and name to address mappings. For instance, the DHCP can use the Dynamic DNS updates mechanism [RFC 2136] to perform the DNS mapping update [15]. Figure 6, does not show the DNS update in detail. The MS sends a SIP REGISTER message whose CONTACT is set to the MS's new address to the visiting registrar (VR) that contains the service profile of the MS. The VR uses the SIP INFO method to send MS's profile to the HR for authentication. The HR responds to the VR with a SIP OK if authentication is successful, otherwise, HR responds with a "603 Decline" response. Then, the VR sends a SIP OK to the MS to confirm its registration with the visiting network. Therefore, additional requirements for supporting this registration approach are the followings.

- The DHCP SHALL interact with the DNS and update it dynamically.
- The SIP INFO method SHALL be able to convey the question "Is profile [....] valid? " to the HR in the method message body.



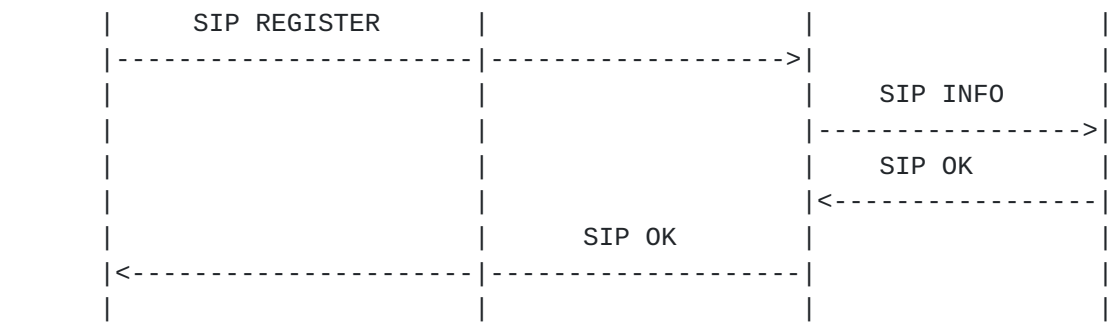


Figure 6. The signaling flow for the registration: Approach 1

Assuming that the processing time is negligible, the maximum registration time using this approach equal to sum of the round trip (MS-DHCP-MS), the round trip (MS-VR-MS), and the round trip (VR-HR-VR) delays. The first term represents the time it takes to get a new address, the second and third is the registration time. The registration time comprises the time for mobile's interaction with the SIP registrar as well as the time it takes the VR to communicate with the HR in order to authenticate the mobile.

In order to reduce the impact of roaming on the performance of interactive real-time services, it is essential to minimize the registration time of a mobile in a visiting network. As Figure 6 indicates this goal can be achieved through minimizing the mobile authentication time as well address acquisition time. The mobile authentication can be expedited through replicating a mobile's profile in networks that are most likely to be visited by the mobile [13]. This profile replication reduces the registration time by a VR-HR-VR round trip, though it increases the control load due to profile administration, and its effective realization requires continuous monitoring of user's mobility patterns. An approach that augments the SIP registrar with DHCP functions and reduces the address acquisition time is described in Section 4.1.2.

4.1.2 Registration: Approach 2

In a nutshell, this approach equips the SIP registrar with DHCP functions so that the address acquisition time is reduced. Realization of this approach requires the modification of SIP REGISTER method so that if the CONTACT field is set to a default registration/hand-off (i.e., "RHO") value , the SIP registrar (i.e., registration server) shall also ask for a temporary address for the mobile. The registrars shall be equipped with a DHCP client as well as shall be co-located with a DHCP server that allows it to assign IP addresses to the mobiles. This registration algorithm operates as follows:

+ The mobile uses a SIP REGISTER method with CONTACT = "RHO" to re-register as well as get it a new address. When the visiting registrar (VR) receives this message
  - the VR assigns a new temporary address to the mobile, i.e., its DHCP client ask for an address from its DHCP server,
  - the VR and HR interact to authenticate the mobile, if the authentication fails, VR sends a 603 Decline message to the mobile, otherwise,
    * the VR DHCP server updates the DNS, and
    * the VR send the temporary address to the mobile in the 200 response as Contact header field.

Assuming negligible processing time, the maximum registration time equals the sum of the round trip (MS-VR-MS), and round trip round trip (VR-HR-VR) delays. Like approach 1, a profile replication method may be used to eliminate the round trip delay (VR-HR-VR) involved in authentication, and minimize the registration time. The key advantages of this scheme (compared to approach 1) are that it

a. reduces the address acquistion time becuase the registrar itself can assign new address, and
b. protects network resources against fraud because the registrar authenticates the MS before sending the MS its new assigned address.

The signaling flow of this registration procedure is shown in Figure 7. Note that Figure 7 does not depict DNS update process in detail.

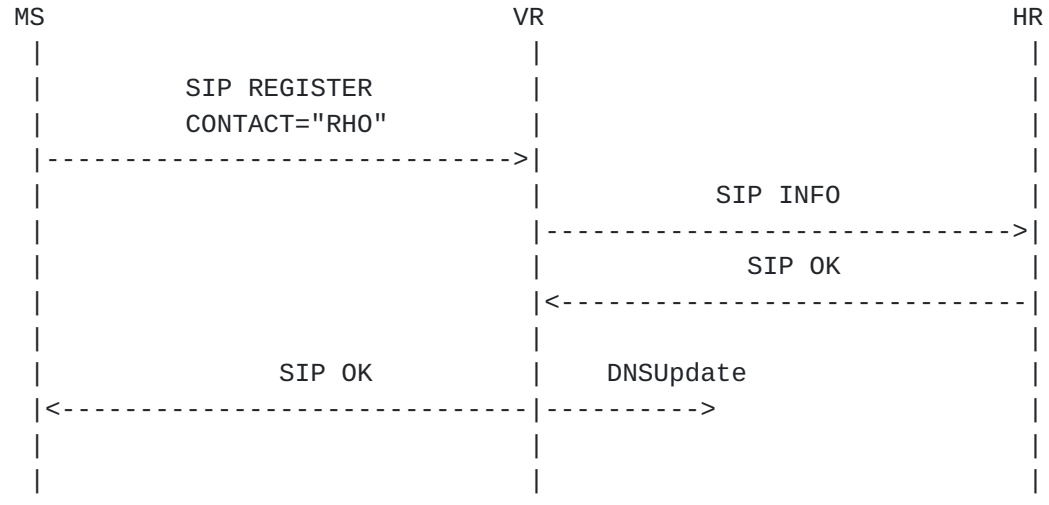


Figure 7. The signaling flow for registration: Approach 2

The followings are additional requirements for supporting this registration approach with SIP.

** The SIP REGISTER method SHALL designate a "RHO" CONTACT that allows the registrar to obtain a new address from the DHCP on behalf of the mobile.
** The DHCP sever of VR SHALL either update the DNS dynamically or a new protocol be developed to allow applications to use SIP registrar for name to address and address to name mappings.

An interesting question is how does the SIP registrar inform the mobile about its new address? The answer is exactly the way DHCP does it. The TCP(UDP)/IP software should accept and forward to the IP layer any IP packets delivered to the mobile's hardware address before its IP address is configured. The SIP registrar may use the limited broadcast IP address to force the IP layer to broadcast the registrar's response on the subnet so that it is delivered to the mobile's hardware address before the TCP(UDP)/IP software of the mobile is configured. If mobiles can accept hardware unicast datagrams before their TCP(UDP)/IP software are configured, the registrar may use this capability to deliver the mobile's new/temporary address.

I believe the fact that VR is equipped with DHCP client and server capabilities is consistent with RFC 2543 requirement that explicitly states a SIP registrar cannot act as a SIP client. However, this point should be examined further.

4.2 Mobility Support

The mobility support comprises two functions, i): location service, i.e., locating mobile users in response to new incoming session requests, and ii): hand-off, i.e., ensuring soft hand-off as the mobile user roams across subnets and/or domains. What follows describes how HMMP uses SIP to support these functions.

4.2.1 Location Service

The mobile has moved to a new location when a corresponding host initiates a session. In this case, HMMP sets up the session as follows:
- The corresponding host invites the mobile station (i.e., MS),
- A SIP redirect server (SIP-RS) answers that the mobile is moved to a new location (i.e., temporary address),
- The corresponding host re-invites the mobile at the temporary address, and
- a session is set up between the corresponding and mobile hosts, and the data transfer begins.

Figure 8 depicts the signaling flow for location service.

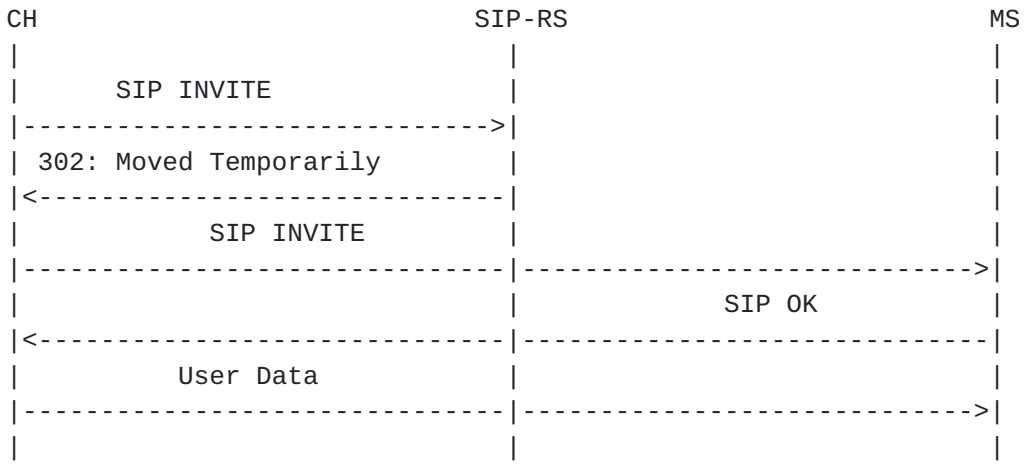


Figure 8. The signaling flow for location service

The corresponding host sends a SIP INVITE message to the mobile station. A redirect server that has intercepted the INVITE message sends a 302 (i.e., moved temporarily) redirection message to the corresponding host with the mobile's new/temporary address as its Contact header field. The corresponding host sends a SIP INVITE message to the new address, the mobile responds with a SIP OK, and the data transfer begins. Since the DHCP dynamically updates the DNS mappings, new TCP connections are established using the most recent IP address of the mobile.

4.2.2 Hand-off

To ensure soft hand-off, HMMP should re-establish a new session between the corresponding host and the mobile station (MS) at its new location, and create a short-lived tunnel for forwarding the transient data of the session to the mobile station's new location. When the MS moves to a new location during the session, The MS re-registers (using either of registration methods described in Section 4.1) and obtains a new address. Then, HMMP provides means of hand-off as follows:

+ A new session with the same session ID is created between corresponding host (CH) and the mobile. In order to create a new session, the MS (or SIP server) re-invites the corresponding host to the new address of the MS.
+ The MS or SIP server uses the SIP INFO method to create a short-lived tunnel between the previous MSC and the new MSC to reduce the loss of session transient data. In order to create the tunnel
  - The MS or SIP server sends an INFO message to the previous MSC (P-MSC) which is the same as the default gateway of the MS before getting its new address, and

- binds the old address of the mobile with its new one, so that transient messages are forwarded to the new address of the MS, and packet loss is reduced. The expire filed of the INFO method is used to specify the tunnel lifetime (i.e., a time-out period after which the tunnel is discontinued). The exact algorithm for determining the tunnel lifetime requires further study.

+ The MS SIP user agent also sends an INFO message to the SIP user agent of any corresponding host whose address is in the MS's SIP-EYE record of ongoing TCP connections so that each corresponding host binds the original IP address of the MS to its current (i.e., new) IP address.

Note that the P-MSC uses IP encapsulation [19, 20] to create a tunnel for forwarding the transient packets to the mobile's new location. The key requirement for the realization of the tunneling process is that each MSC SHALL have a SIP user agent. The signaling flow for hand-off is shown in Figure 9.

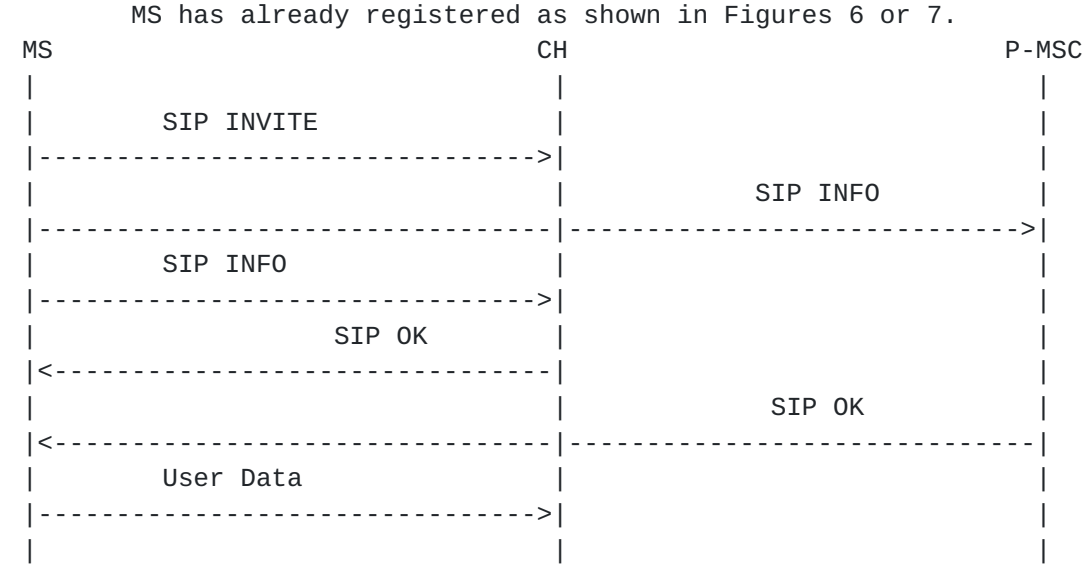


Figure 9. The signaling flow for hand-off

It is worth noting that Figure 9 shows an instance of the signaling flow for hand-off. The exact sequence of SIP OK responses from the P-MSC and CH SIP user agent to the MS SIP user agent depends on the round trip delay between these entities as well as the network traffic these messages encounter as they traverse the network. In summary, additional requirements for supporting hand-off are the following.

- The SIP user agent SHALL be equipped with a SIP_EYE agent that tracks TCP connections in the MS. - The SIP_EYE agent SHALL maintain a state comprising the <original MS

IP address, previous MS IP address, current MS IP address, original corresponding host IP address> per TCP connection within the SIP user agent of the MS. - The SIP user agent SHALL keep the address of the last default gateway (i.e., previous MSC) before hand-off). - The SIP user agent SHALL understand address binding INFO messages and take necessary actions. - The SIP INFO method SHALL support address bindings, i.e., understand a "Bind [address 1] to [address 2] " instruction in the method message body.

5. The SIP_EYE Agent

The whole premise of the SIP_EYE agent is to ensure that HMMP supports TCP as is without any modifications to TCP. SIP_EYE SHALL be a simple TCP tacking/monitoring agent with small footprint residing within the SIP user agents of mobile stations (MSs) and corresponding hosts (CHs). Its functions are to

a) identify and track ongoing TCP connections of a mobile station, and
b) maintain a list of ongoing TCP connection identifiersand their respective corresponding hosts so that the SIP user agent of the mobile sends them INFO messages to bind the original IP address of the mobile with its current one.

The SIP_EYE agent tracks both the transmitted and received TCP packets concurrently to create and update the list of ongoing TCP connections in the MS. It runs two concurrent monitoring and updating processes, one for tracks the transmitted packets, and the other received ones. The role of SIP_EYE in hand-off of TCP connections has already been discussed in detail. The following pseudo-code describes the basic TCP tracking operation of the SIP_EYE agent for the simplest case.

```
// SA: Source address of a packet.
// DA: Destination address of a packet.
// SYN: Synchronization code bit
// ACKB: Acknowledgment code bit
// FIN: Sender end of byte stream code bit
// SEQ: Sequence number
// ACKN: Acknowledgement number

// Auxiliary variables
//  CL_ID: Connection Label ID
//  STAT: Connection Status
//     STATUS takes values, Setup_Req, Setup_Prog, Established,
//     Release_Req, Release Ack, Release Accpet, Disconnect)
```

```
      //
      // The TX SIP_EYE Entity.

   for (;;) {
                Capture the header of transmitted TCP packets;
      if (SYN = 1 & ACKB = 0) {
       Add a TCP entry as follows to the temporary list of connections
            <    original MS IP address = SA;
                 previous MS IP address = SA;
                 current MS IP address = SA;
                 original corresponding IP address = DA;
                 CL_ID = SEQ;
                 STAT = Setup_Req; >
                 }
       else if (ACKB = 1 & SYN =0) {
         Get the STAT of the TCP entry,
               < original MS IP address = SA;
                 previous MS IP address = SA;
                 current MS IP address = SA;
                 original corresponding IP address = DA;
                 CL_ID = ACKN-1;
                 STAT  =   **; >
                 if  ( STAT = Setup Prog ) Set STAT = Established;

       // A TCP connection is added to the table of ongoing connections.
                 if else (STAT = Release_Ack) {
                 Set STAT = Disconnect;
                 Remove the TCP entry from the table of ongoing connections.
                 }
                 else
                 Error!;
         }
       else if { ACKB =1 & FIN = 1 ) {
        Reset the CL_ID and STAT of the ongoing TCP entry,
        < original MS IP address = SA;
          previous MS IP address = previous MS IP address;
          current MS IP address = current IP address of the mobile;
          original corresponding IP address = DA;
          CL_ID = ** ;
          STAT = Established; >
       to
          CL_ID = SEQ;
          STAT = Release_Req;
         }
    }
```

```
        // The RX SIP_EYE Entity. It is similar to TX entity and they
        // both run concurrently to manage a single TCP connection list.

   for(;;) {
      Capture the header of  received TCP packets;
        if (SYN = 1 & ACKB = 1) {
          Reset the STAT of the TCP entry ;
          < original MS IP address = DA;
            previous MS IP address = DA;
            current MS IP address = DA;
            original corresponding IP address = SA;
            CL_ID = ACKN-1;
            STAT = Setup_Req; >
      to
            STAT =  Setup_prog;
            }
        else if (SYN = 0 & ACKB =1) {
          Reset the STAT of  TCP_entry;
           < original MS IP address = DA;
             previous MS IP address = DA;
             current MS IP address = DA;
             original corresponding IP address = SA;
             CL_ID = ACKN-1;
             STAT = Release_Req; >
       to
             STAT = Release_Ack;
         }
         else if { ACKB =1 & FIN = 1) {
         Reset the STAT of TCP entry
           < original MS IP address = DA;
             previous MS IP address = previous MS IP address;
             current MS IP address = current IP address of the mobile;
             original corresponding IP address = SA;
             CL_ID = ACKN-1;
             STAT = Release_Ack; >
      to
             STAT = Release_ACK;
          }

     }

       // Update of ongoing TCP connection list upon hand-off.
       // new  MS IP address: The new address that has been assigned to the
       // mobile upon hand-off.

   if (hand-off) {
     while (!eof ongoing list) {
     <  original MS IP address = original MS IP address;
```

```
        previous MS IP address = current MS IP address;
        current MS IP address = new MS IP address;
        original corresponding IP address = original corresponding IP address;
        CL_ID = **;
        STAT = Established;
      }
```

The preceding pseudo-code describes the basic operation of SIP_EYE in an environment whose packet error or loss ratio is negligible and no connection set-up message of TCP is lost or corrupted. It shall be refined further so that it becomes robust enough for use in a wireless environment that has relatively (compared to wireline networks) high packt loss and error and TCP set up messages may be lost or corrupted. Furthermore, the interactions of the SIP_EYE agent with the entities of current SIP user agent as well as its integration within the SIP user agent require further study.

6. Impact of Mobility on SIP Specifications

Having described HMMP, let us summarize requirements for supporting mobility on SIP via HMMP or other protocols. The requirements are the following.

** The SIP INFO method SHALL be able to convey the question, "Is the profile [....] valid? ", to the HR in the message body of INFO method.
** The SIP INFO method SHALL support address bindings, i.e., understand a "Bind [address 1] to [address 2] " instruction in the message body of the INFO method.
** The SIP REGISTER method SHALL designate a "RHO" CONTACT that allows the registrar to obtain a new address from the DHCP on behalf of the mobile.
** The SIP user agent SHALL be equipped with a SIP_EYE agent that tracks TCP connection.
** The SIP_EYE agent SHALL maintain a state comprising the <original MS IP address, previous MS IP address, current MS IP address, original corresponding IP address> per TCP connection.
** The SIP user agent SHALL keep the address of the last default gateway (i.e., previous MSC) before hand-off).
** The SIP user agent SHALL understand address binding INFO messages and take necessary actions.
** The DHCP sever of VR SHALL either update the DNS dynamically or a new protocol be developed to allow applications to use SIP registrar for name to address and address to name mappings.

Except for the interaction between DHCP and DNS, SIP specifications SHALL support other functions/requirements so that SIP can support

signaling needs of roaming users in 3G-IP networks.

7. Summary and Open Issues

This document has presented the preliminary specifications of HMMP, and identified the impact of mobility on SIP and proposed necessary extensions to ensure that SIP can support roaming users adequately. HMMP is a protocol that supports real-time and non-real-time multimedia applications on mobile terminals of 3G-IP networks. HMMP utilizes as well as extends session initiation protocol (SIP) to provide means of domain hand-off (i.e., roaming), and subnet-off (i.e., macro mobility) so that users can access the network from any location using their own mobile terminal. HMMP can spoof constant endpoints for mobile TCP connections and supports mobile TCP applications without any changes to the TCP. Among the open issues that may influence SIP specifications and require further study are:

-- the specifications of a resource reservation mechanism for supporting real-time multimedia applications of roaming users in a 3G-IP network whose signaling system is built on SIP,
-- the extension of the SIP_EYE specifications so that it is able to account for error in and loss of the TCP connection set-up packets, and to interact and co-operate with the current SIP user agent as defined in RFC 2543,
-- the specifications of AAA entity, and
-- interworking with the PSTN.

8. Acknowledgments

The authors wish to acknowledge the contributions of other members of the ITSUMO(TM) team from Telcordia (P. Agrawal, , S. Das, D. Famolari, A. McAuley, P. Ramanathan, and R. Wolff) and Toshiba America Research Incorporated (T. Kodama).

(TM): ITSUMO (Internet Technology Supporting Universal Mobile Operation) is a trademark of Telcordia. It is a joint research project of Telcordia Technologies and Toshiba America Research Inc. (TARI). It envisions an end-to-end wireless/wireline IP platform for supporting real-time and non-real-time multimedia services in the future. Its goal is to use IP and third generation wireless technologies to design a wireless platform that allows mobile users to access multimedia services on a next generation Internet. In Japanese, ITSUMO means anytime, always.

9. References

1. D. Barboza, "Motorola and Sun to Build Joint System for Net

Access", The New York Times, June 10, 1999.

2. Cnnfn Industry Watch, "NOKIA: Industry leaders for focus group to promote third generation wireless IP Technology", June 11, 1999.

3. Telcordia Technologies, "Voice Over Packet in Next Generation Networks: An Architectural Framework", Bellcore SR-4717, Issue1, January 1999.

4. ITU-R Rec. M.687-2, "International Mobile Telecommunications-2000 (IMT-2000)", 1997.

5. ITU-R Rec. M.817, "International Mobile Telecommunications-2000 (IMT-2000)", Network Architectures", 1992.

6. ITSUMO Group, "Evolution of Wireless Telephony towards Voice over 3G-IP", 3GPP2- P00-19990824-010, August 23, 1999.

7. ITSUMO Group, "A Service Profile for 3G-IP Wireless Networks", 3GPP2-P00-19990927-009, September 27, 1999.

8. ITU-R Rec. M.816-1, "Framework for Services Supported on International Mobile Telecommunications-2000 (IMT-2000)", 1992.

9. IETF, "SIP: Session Initiation Protocol", RFC 2543, March 1999.

10. IETF, "SDP: Session Description Protocol", RFC 2327, April 1998.

11. IETF, "Dynamic Host Reconfiguration Protocol", RFC 2131, March 1997.

12. S. Donavon, "The SIP INFO Method", <draft-ietf-mmusic-sip-info-method-01.txt>, work in progress, June 1999.

13. D. Lam, Y. Cui, D.C. Cox, and J. Widom, "A Location Management Technique To Support Lifelong Numbering in Personal Communications", January 1998.

14. A. McAuley, S. Das, and S. Baba, Y. Shobatake, "Dynamic Registration and Configuration Protocol for Mobile Hosts", <draft-itsumo-drcp-00.txt>, work in progresss, October 1999.

15. Y. Rekhter, and M. Stapp, "Interaction between DHCP and DNS", <draft-ietf-dhc-dhcp-dns-10.txt>, work in progress, June 1999.

16. E. Wedlund, and H. Schulzrinne, "Mobility Support using SIP", ACM Multimedia Workshop, Seattle, August 1999.

17. IETF, "IP Mobility Support", RFC 2002, October 1996.

18. C. Perkins, and D. B. Johnson, "Route Optimization in Mobile IP", <draft-ietf-mobileip-optim-08.txt>, February 25, 1999.

19. IETF, "IP Encapsulation within IP", RFC 2003, October 1996.

20. IETF, "Minimal Encapsulation within IP", RFC 2004, October 1996.

21. IETF, "Resource reSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, September 1997.

22. DCS Group, "Integration of Resource Management and Call Signaling for IP Telephony", <draft-dcsgroup-mmusic-resoure -00.txt>, work in progress, August 1999.

10. Authors' Addresses

Faramak Vakil
farm@research.telcordia.com
Telcordia Technologies, Rm 1C-135B,
445 South Street, Morristown, NJ 07960-6438.

Ashutosh Dutta,
adutta@research.telcordia.com
Telcordia Technologies, Rm 1B-217B
445 South Street, Morristown, NJ 07960-6438.

Jyh-Cheng Chen,
jcchen@research.telcordia.com
Telcordia Technologies, Rm 1G-236B,
445 South Street, Morristown, NJ 07960-6438.

Shinichi Baba
sbaba@tari.toshiba.com
Toshiba Research America Inc. (TARI)
P. O. Box 136
Convent Station, NJ 07961-0136

Yasuro Shobatake
yasuro.shobatake@toshiba.co.jp
Toshiba Research America Inc. (TARI)
P. O. Box 136
Convent Station, NJ 07961-0136