Simple Mobile IP (SMIP)

Status Of This Memo

This document describes an alternative to the support for IP mobility compared to the solution outlined and specified in [MobIP]. As the title of the solution implies, it addresses the problems with the overall complexity of the current Mobile IP solution including some of the proposed extensions as outlined in [RouteOpt], [3G-IMT]. This more simplistic approach relies on two basic prerequisites: Development made in recent years, and also development foreseen in a near-term future, regarding certain key protocols and techniques for name-to-address resolution, directory services, address assignment, and roaming support; and also the fact that the solution is suited for usage within one organizational scope.
1.0 Introduction

The support for IP mobility as specified in [MobIP] relies on the concept of home agent (HA) and foreign agent (FA). The home agent resides on the same IP subnet as the mobile terminal (MT) is normally connected to, and a foreign agent resides on subnets which mobile terminals may visit. Through the use of a fixed IP address and a care-of address assigned to the MT, the user may connect its terminal to some other subnet besides the subnet which the terminal is normally connected to. IP packets destined for the MT will be forwarded by the HA to the FA and then finally to the MT (by means of tunneling). Packets from the MT can be sent directly towards its destination.

The solution has several drawbacks (some just a result of evolving technologies, no offense):
- triangular routing, i.e. asymmetric routing with respect to topology
- inefficient use of link resources through the use of tunneling which may span a large number of router hops
- support for QoS is not straightforward with triangular routing
- inefficient use of network resources through non-optimal routing
- the use of a fixed (and public) IP address, which is not the normal case in today's Internet and intranets

To address at least some of these drawbacks, one basically has to look for a more symmetric and distributed solution, possibly as similar as possible as the solution in use for fix terminals, with the addition of the need for support for mobility. It is also then possible to let the solution rely on existing protocols, or protocols/technologies under development. In this context, it is important to distinguish between session mobility and user mobility:

Session mobility: Applications and TCP sessions will not be affected by the fact that the terminal is moving within and between subnets, except for some packet loss which may result out from a handover between radio base stations.

User mobility: A user of an MT which may get connected to a subnet within the context of an administrative domain, e.g. an intranet.

For datacom-type of applications, e.g. Web browsing, the requirement is to support session mobility throughout a geographical area which has continuous radio coverage. Typical examples of such areas are buildings, campuses, and public "hot spots" like hotels, conference centers, airports.

Regarding user mobility, the requirement is that it doesn't need to be better than what is supported for fix terminals, though it should be noted that mobile terminals may drive the need for increased support for user mobility. The latter becomes more and more evident with the introduction of nomadic computing and the nomadic office. Clearly, this means that the notion of "home" and "foreign" don't make sense anymore. As a consequence, those concepts have been removed and instead been renewed in this memo.

This background, prerequisites, and requirements, is the foundation for the solution outlined in this memo.

Johnsson
Expires September, 1999
[Page 2]
2.0 A reference model

The following reference model is referred to in the following sections describing the protocol layout and basic procedures.

```
+-----------+   +---+  +-----+        +-----+
| Application|   | RBS|  | LR  |        | MER |
| Transport |   |     | Fixed LAN |        |     |
| IP-MLAN |   |     |             |        |     |
| IP-LLAN |   |     |             |        |     |
| Link |   |     |             |        |     |
| Physical |   |     |             |        |     |
```

FIGURE 1. SMIP Reference Model

A Mobile Terminal (MT) connects to a LAN through the Radio Base Station (RBS) via the air interface, e.g. Hiperlan 2 or 802.11. The RBS functions as a bridge on the LAN. The Local Router (LR) routes packets to/from the subnet which the MT is currently connected to. The Mobility-Enabled Router (MER) is a router handling routing packets to and from Mobile LANs (MLAN). Each MT is connected to an MLAN as well as a local LAN. Thus, an MT has two IP addresses for one network interface (the air interface in this case); one reflecting connectivity to the local LAN handled by LR, and one IP address reflecting connectivity to the MLAN. An LLAN may have both wireless and fixed hosts connected to it, while an MLAN only has wireless hosts connected.

As the MT is moving, the connectivity towards the local LAN is changing, and thus also the IP address reflecting this change in local LAN connectivity. The IP address reflecting the MLAN connectivity is never changing.

The protocol reference model for the MT is depicted in figure 2 below.

```
+-----------+   +-----------+   +-----------+   +-----------+   +-----------+   +-----------+   +-----------+
| Application|   | Transport |   | IP-MLAN |   | IP-LLAN |   | Link |   | Physical |
```

FIGURE 2. MT protocol reference model.
The two levels of IP are stacked on top of each other, just like IP-in-IP tunneling as defined in [IP-TNL]. As described above and according to the protocol reference model, the transport layer will not experience any change in IP address.

Other protocols of importance for the solution, and which are not shown in figure 2, are DHCP and the optional use of IPsec protocols. The use of these protocols will be further detailed below.

3. Protocols and procedures

3.1 Bootup phase

In the bootup phase, it is proposed that the MT acquires the two IP addresses needed for the two IP layers, IP-MLAN and IP-LLAN, by means of extensions through a set of new options to DHCP.

During the bootup phase, the MT will also retrieve information via DHCP about the address of the MER handling the MLAN to which the MT is connected to.

3.2 IP packet handling

3.2.1 IP packet handling at the MT

The transport layer will submit packets for transmission to IP-MLAN. IP-MLAN will set the source IP address to the address corresponding to the IP address of the MLAN, and the destination IP address to the address of the packet’s final destination. IP-MLAN will in turn submit the IP packet to IP-LLAN. IP-LLAN will set the source IP address to the address corresponding to the IP address of the LLAN, and the destination IP address to the address of the MER. Finally, the address is submitted to the link and physical layers for transmission over the local LAN.

Upon reception, IP packets from the physical and link layers are delivered to IP-LLAN. The contents of the IP header is checked to specifically verify that the source IP address is the address of the MER. The IP header for the IP-LLAN layer is then stripped off, and then the contents left of the packet is delivered to the IP-MLAN layer. The IP-MLAN strips off the IP header of this layer, and finally the packet is delivered to the transport layer.

3.2.2 IP packet handling at LR

Packets from the MT will be routed to the MER by LR as indicated by the IP destination address.

Packets to the MT will be routed onto the local LAN which the MT is connected to.
3.2.3 IP packet handling at MER

MER will receive packets from MTs destined for the MER itself. MER strips off the IP header of this packet, and then uses the information in the IP header related to MLAN for purposes of routing the packet to its final destination.

Packets received by the MER with an destination IP address associated to an MT on an MLAN, will be encapsulated into an IP packet. The source IP address is set to the address of MER, and the destination IP address to the address of the MT pertaining to the local LAN which the MT is currently connected to.

3.3 IP mobility handling

As the MT moves, a shift may occur with respect to the connectivity to the local LAN. It is currently out of the scope of this memo how an MT discovers that a shift is underway with respect to LLAN. But for example, the protocols at the air interface may include protocol support for indicating this shift in connectivity. The current version of this memo only deals with the handling of the IP connectivity and the correlation between MLAN and LLAN, and also the necessary change of IP address at the IP-LLAN level due to change in LLAN connectivity.

3.3.1 IP connectivity

As with fixed terminals, there is no need to advertise connectivity between an MT and a router on a LAN (LR and MER in the SMIP case).

3.3.2 MLAN - LLAN correlation

To enable correct routing of messages from the MER towards an MT, the MER must at each instance of time know the current location of the MT, i.e. to know which LLAN the MT is currently connected to. Due to a possible movement of the terminal, this connectivity may change over time. Thus, the MER must receive indications about an MT’s current location.

It is proposed that the MLAN - LLAN binding has limited lifetime, and thus the binding must be periodically refreshed to avoid timer expiration. In addition, it is also proposed that the MT triggers an update of this binding to the MER whenever a change in this mapping occurs. If the timer expires, the mapping shall be removed by the MER, and MER shall treat the MT as being unreachable.

This memo proposes to use an extension to ICMP for handling of IP connectivity and correlation between MLAN and LLAN. The procedure of using an ICMP message for this purpose, is to send an ICMP both periodically and triggered according to the above description.
3.3.3 IP address for LLAN connectivity

Due to the movement of the MT, LLAN connectivity may change, and thus the IP address reflecting this connectivity.

It is proposed that when the MT receives an indication that an handover between RBSs results in that the MT moves from one LLAN to another, the MT requests a new IP address for the LLAN level by means of a possible set of new options to DHCP.

3.3.4 Moving out and within radio coverage

An MT may temporarily be moved out of the range of radio coverage from RBSs, and later once again be moved within the range of radio coverage. This is similar as unplugging and then replug a fix terminal to a LAN.

When an MT detects that it once again is connected to a local LAN, it is proposed that the MT reinitiates DHCP requests for the two IP addresses reflecting connectivity towards an LLAN and an MLAN. This may in turn lead to that the MT will be assigned new IP addresses for one or both of the two IP levels. DHCP may need to be extended with a set of new options to support this scenario.

3.4 Security support

IPsec protocols such as the Authentication Header and the Encapsulating Security Payload defined in [AH] and [ESP] respectively, may be inserted between the two IP headers of the IP-LLAN and IP-MLAN levels. The rules that govern the use of IPsec protocols shall comply to the IPsec protocol suite of recommendations when using IPsec in tunnel mode of operation.

Other security mechanisms may be supported as well, for instance on the transport level, but that is outside the scope of this memo.

3.5 ARP and broadcasts

As the MLAN is "virtual" in the sense that the mapping between the logical and physical structure of the MLAN is not one-to-one, e.g. it may include router hops, the Address Resolution Protocol as defined in [ARP] shall not be used. It shall also be specifically noted that for clarity and consistency the MT shall be, with respect to addressing, associated to the address of the IP-MLAN level. This results in that all traffic to/from an MT must pass through the MER.

But, for the purpose of conserving bandwidth, and to make most efficient use of network resources, ARP may be used to forward traffic directly between the source and the destination hosts, iff they are located on the same LLAN. In this case, the IP-LLAN protocol layer is "empty", i.e. no IP header is added by IP-LLAN.
The asymmetric traits of this option with respect to routing shall be used with great care.

Other forms of broadcasts are sent just as unicast packets encapsulated to the MER, which will retransmit the broadcast encapsulated in unicast packets to all MTs on the MLAN.

### 3.6 Multicast

In IP, the Internet Group Management Protocol as defined in [IGMP] is the foundation for group membership registration. A host reports group membership to its local router by responding to group membership queries. The important characteristic to note about IP multicast in this scope of work, is that it is receiver-oriented, meaning that IP multicast addresses indicates a set of destination hosts, i.e., those being members of a certain group. It has nothing to do with the source host, unless this the source host as well.

With respect to mobility, the IP multicast paradigm is well suited to serve also this aspect of connectivity, as both IGMP and the different routing protocols for multicast rely on the soft state concept. As a result, the graph of the distribution tree for a multicast group adapts depending on the current locations of group members.

#### 3.6.1 Receiving multicast

The discussion above results in that an MT with respect to IP multicast, and traffic directed towards MT (i.e., MT is a group member), works exactly the same as for fixed terminals. This means that the IP-MLAN layer is "empty" in this direction of traffic.

One issue though may arise in the event of IGMP version 3 [IGMPv3]. In this case, a member may indicate from which sender(s) the member host is willing to receive IP multicast packets from. This may lead to the need for specifically indicating the very source of a membership report, which then must correspond to the address of the IP-MLAN. This is still for further study.

#### 3.6.2 Transmitting multicast

When transmitting multicast packets, the source of the packets must equal the address of the IP-MLAN level, for reasons of consistency. Thus, IP multicast packets are transmitted in the same way as unicast packets described above in section 3.

This may lead to non-optimal distribution trees for IP multicast, especially for those members which are nearer to the MT source than the MER. Possible work-arounds or alternative solutions can quite easily be deduced, e.g., snooping into tunneled datagram or shortcutting the IP-LLAN level, but this is for further study.
An alternative option would be to transmit the multicast packets unencapsulated, i.e. by shortcutting the IP-LLAN level.

4. Miscellaneous

4.1 DNS

The DNS will resolve to addresses corresponding to the IP-MLAN level. Regarding the IP-LLAN level, this address is invisible to DNS.

4.2 DHCP servers and MER/MLAN relation

The DHCP servers will through the responses back to the MT, give proposal(s) as to which MER the MT can use and establish connectivity. The proposal should preferably be based on the current location of the MT, i.e. LLAN connectivity, and what MER(s) that are available in the "neighborhood" of MT’s current location. Proposals on MER may also be based on some estimate of how the MT may move around, which results in some kind of judgement of tradeoffs based on routing performance, QoS, etc.

This is not part of the current scope of this memo to define any algorithms or rules, that can be used to decide upon appropriate proposal(s) on MER(s). For the time being, it will be up to the management of DHCP servers to configure appropriate MER proposals.

4.3 QoS

QoS is a difficult and still pending issue also for fixed terminals, and becomes emphasized and highlighted for mobile terminals. On the IP layer, an MT may make use of either of the two proposed solutions for QoS provisioning defined as of today: Integrated Services using RSVP or Differentiated Services (DiffServ) using the DS field in the IP header.

The main issue in SMIP as outlined in this memo, is the IP tunnel between the MT and the MER, and of course the fact that the terminal is mobile.

Regarding RSVP, [RSVP-Tnl] describes how end-to-end RSVP sessions map to tunnel sessions. Due to the aspect of a mobile terminal, the reservations for the tunnel between the MT and the MER must be created dynamically on demand, which is outlined as one of the options in [RSVP-Tnl].

Regarding DiffServ as defined in [DiffServ], there are no specific rules as how to perform mapping of a service indicated by the DS field between an end-to-end service and the service for a tunnel. This will be a matter of local policies.
4.4 Handover between MERs

It could be envisaged that the need for session mobility should be extended beyond the limitation of connectivity to one MER, meaning that a "handover" would be performed from one MER to another, possibly leading to a change in MLAN connectivity, depending on how to solve this form of mobility. The support for session mobility between MERs is for further study.

5. Notice Regarding Intellectual Property Rights

Ericsson may seek patent or other intellectual property protection for some or all of the technologies disclosed in this document. If any standards arising from this disclosure are or become protected by one or more patents assigned to Ericsson, Ericsson intends to disclose those patents and license them on reasonable and non-discriminatory terms. Future revisions of this draft may contain additional information regarding specific intellectual property protection sought or received.

6. References


[AH] : IP Authentication Header, S. Kent et al, RFC 2402


[DiffServ] : An Architecture for Differentiated Services, S. Blake et al, RFC 2475


[Route-Opt] : Route Optimization in Mobile IP, C. Perkins et al, Work in Progress

[RSVP-Tnl] : RSVP Operation over IP Tunnels, A. Terzis et al, Work in Progress
7. Authors’ Address

Martin Johnsson
Ericsson Radio Systems
Wireless LAN Systems
Esplanaden 3C
SE-164 80 Stockholm, Sweden
Martin.Johnsson@era.ericsson.se