INTERNET DRAFT   Hossam Afifi
                                                        INRIA Sophia
June 20,1999   Jim Bound
expires December 20, 1999   Compaq Computer
Corporation <draft-afifi-sixtel-00.txt>
Scott Cadzow

                                                         Cadzow 3C
                                                      Laurent Toutain
                                                       ENST Bretagne

             Support of IPv6 over Cellular Communications Systems (6Tel)

Status of this Memo

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

Abstract

   We propose an architecture for the support of IPv6 over cellular mobile
   networks. The architecture is adapted to the characteristics of global

cellular systems offering connectivity to very large numbers of subscribers
(e.g. 3GPP). We are also concerned with particularities of the cellular air
interfaces. The architecture takes in consideration   mobile IPv6
terminals. Finally, it gives a way of protection of the available network
resources and of the subscribers confidentialities with an on demand
security mechanism.

   First an addressing scheme based on the AGGR address structure and E.164
numbering structure is presented. This addressing scheme is independant
from the terminal mobility and hence does not involve any Mobile IP address
management. We describe the mechanisms involved in the communication from
a Global cellular system to the fixed network and vice versa, and within
the Global cellular system. We describe the necessary procedures for ARP
resolution, DHCP and bandwidth reservation in coordination with the Link
Layer management modules (Mobility Management, Call Management).

[1]. **Introduction**

Cellular systems architecture is composed of several sub-systems. The
mobile station (MS) is the terminal device. It is identified by a
manufacturer unique code and by the user code present in the SIM card that
has a direct correspondance with a telephon number called MS-ISDN. The
base station (BSS) groups the infrastructure equipments handling radio
aspects and the wired connections to the rest of the network. A mobile
switching center (MSC) is an entity responsible for co-ordinating call
setup and mobility management. It is a rather big equipment that controls a
number of BSSs and their users (data held in a database called VLR). The
home information about users profiles are held in HLRs (home location
registry). The architecture comprises four main functionalities besides
transmission.

 - The communication management (CM) is responsible for call setup, call
control (exchange with different databases), supplementary services (where
a user can control the services he owns) and short messages services (for
mail messages).

 - Operation, administration and management enables the operator to manage
the system components.

 - Radio Ressources management is the establish circuits by the terminal
with the base station.

 - Mobility Management is the necessary set of operations to handle hand-
overs between MSCs and to implement security functions.


```
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |  OAM        | Connection Mgmt.  |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
        |             |  Mobil. Mgmt.     |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
           |                | Radio Ressource  |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
           |                       Transmission  |
        +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Audio is transmitted through (RR) channels upto the MSC where it is either
routed to another mobile or transformed into a 64kb/s digital signal to the
PSTN.

Sixtel is an architecture for the efficient support of IPv6 in mobile
terminals for data transfers (that could also be voice). The main idea is
to consider the mobile network as a layer two network up to the MSC. In
contradiction with previous data service over GSM (GPRS [7]) the IPv6 cloud
will reach the mobile architecture up to the MSC. It will be considered as
a router. IPv6 will not penetrate further in the mobile network because the
rest of sub-systems will be considered as layer 2 equipments. The mobility
is hence taken care of by this layer two sub-system composed of the Mobile
terminal, the BSS and the MSC.

2. Addressing

   We use the AGGR address format to identify mobile terminals with an
address split into two parts. The first gives the prefix indicating the MSC
router and the second identifies the mobile terminal within the MSC
subnetwork. In order to understand the needed structure of addresses we
describe first the E.164 address formats and their relation with mobile
telephone numbers and identifiers.

2.1. Overview

The Global Mobile Cellular Systems offer a very large scale wireless
communication infrastructure. These systems are designed in a way where
E.164 recommendation provides the numbering structure and functionality for
user identification. Although the E.164 number structure is clear it is not
always used in conformance with the standard. Today the current E.164
numbers are more used as names than addresses for routing.

In mobile telephony, there are many identifications for network sub-
systems. As mentionned earlier, a terminal is identified by its
manufacturer number (unique). The user is identified by a telephone number
that is called MS-ISDN and that is similar in its structure to E.164
numbers. This number is publicly available. The user is also
authenticated to the network with a third number called IMSI (located on
the SIM). The IMSI is a number that should never be public since it is used
in authentication procedures. Finally, the network can hold a real E.164
number for routing the calls to the actual location of the user. This last
number is never visible to the users. In the E.164 recommendation a number
is a string of decimal digits that indicates the public network termination
point. It contains the information necessary to route the call to this
termination point either by some of its parts or externally by some mapping
functions.

   In the SixTEL architecture every mobile terminal will be assigned an IPv6
address according to the MSC it is attached to.

          IPv6 address = current MSC prefix + E.164 number

This format helps to isolate the identification of the terminal from its
current location in the wireless network. The address should not give any
additionnal routing information than the MSC prefix. A mobile terminal has
to be able to have several IPv6 addresses to manage mobility and this will
be explained later. Assignement of IPv6 should be strongly coupled to both
registration in the mobile network and mobility. Upon switching on the
terminal it will try to connect in the available cell and should obtain in
the same time a network prefix and its own MS-ISDN number. The procedure
has to be defined with DHCPv6 and integrated in the CM layer.

[3](#). **Mobility Management**

    The approch for handling mobility in this architecture is based on layer
2. As mentioned before the MM layer is responsible for updating the MSC
with the necessary information to keep complete track of the terminal. It
is able to forward the current calls to the new MSC and switch the
necessary radio channels to the new ones in the second cell.

   When a terminal is registered in a cell, it will be configured as
mentioned before with the MSC prefix and with the user's E.164.

```
        +-+--+-+-+-+-+-+--+-+              +-------------------+
        |     Terminal  A    | <------------> |       MSC  A     |
        +-+--+-+-+-+-+-+--+-+              +-------------------+

                                          local routes for
                                          MSC A:
                                          Terminal A
```
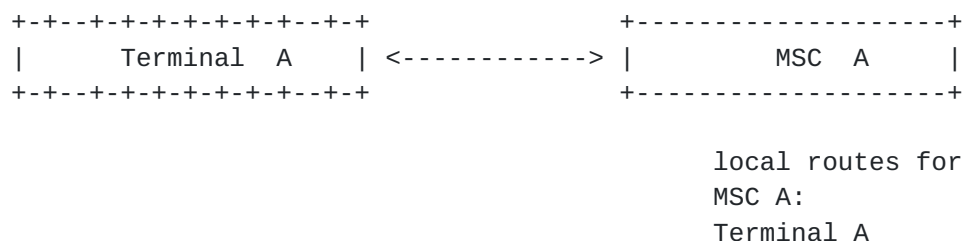
    When the terminal moves from a cell to another within the same MSC
domain, nothing has to change.

When the terminal moves from an MSC (A) to another MSC (B) two cases are
possible:

        a) The terminal is in a sending or receiving mode. This could be
either a call already established or a datagram mode where the terminal is
receiving some packets from another machine.

In this case the terminal will be attributed a second IPv6 interface with
the second prefix. It will however keep its old address until the call or
the state is terminated.

```
          +-+--+-+-+-+-+-+--+-+                +--------------------+
          |      Terminal  A   | <----//------> |       MSC   A     |
          +-+--+-+-+-+-+-+--+-+                +--------------------+
                   .                                     |
                   .                                     |
                   .                           routes:  A send to MSC (B)
                   .                                     |
                   v                                     |
                                                         |
          +-+--+-+-+-+-+-+--+-+                +--------------------+
          |      Terminal  A   | <------------> |       MSC   B     |
          +-+--+-+-+-+-+-+--+-+                +--------------------+

                                               local routes: A'
```
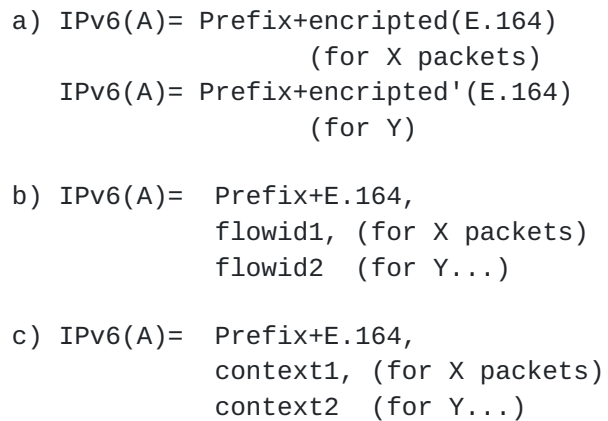
   The configured interfaces should look like:

          > ifconfig -a
                      mo1   prefix (MSC A)+E.164(A)
                      mo2   prefix (MSC B)+E.164(A)

       b) The terminal is not sending or receiving. In this case the first
   address is simply dropped and replaced by the new one belonging to MSC (B)
   domain. As described later, the DNS has to be updated instantaneously.

          > ifconfig -a
                      mo1   prefix (MSC B)+E.164(A)

[4](#). Security considerations and protecting user air interface

 In many situations and according to the service definition of each user,
 it will be probably prefered to prevent any external IPv6 machine from
 sending packets to a mobile terminal especially if the mobile terminal is
 intended for voice over IPv6 only (with real time constrains) unless this
 external terminal is granted for that.

    We define two modes of operation in the SixTel architecture. The first
 is the unsecure mode and it does not need any extra algorithms to be
 implemented. Along with the registration the mobile informs the MSC router
 that it is now available on this sub-network. Whenever a packet arrives
 from another terminal inside or outside the mobile network it is forwarded
 to the terminal.

 The second is a secure mode of operation and requires an additionnal
 encription algorithm. Three alternatives for secured communications are
 possible in this context.

    a) The address is no more in the same format described here-above.
    It is composed of a prefix for the MSC and the cripted E.164 number
 representing the MS-ISDN user number.

```
          IPv6 address = current MSC prefix + encripted(E.164 number)
```

 Whenever a user wishes to establish a secured communication with a new key
it should first advise the MSC in order to remove the old routing entry and
replace it with the new encripted address suffix. In this case, any packet
arriving with the correct suffix will be forwarded to the terminal. If the
suffix is wrong or if it is simply an E.164 number then the packet will be
simply dropped in the MSC router.

   b) The mobile terminal decides for a given session to use a key. This key
will be added to the terminal context in the MSC and should be removed
after that. The key will be inserted in every incoming and outgoing IPv6
packet. This solution does not need any extra encription in the external
IPv6 terminal but only a socket interface that is able to add the flow id
in the packet header.

   c) The last method is the more secure and consists in sending an IPv6
extension in every packet. This however will take some overhead in order to
check every packet and to fetch for the extension.

```
       +-+--+-+-+-+-+-+--+-+            +-------------------+ <----> Y
       |      Terminal  A    | <----->  |        MSC        | <----> X
       +-+--+-+-+-+-+-+--+-+            +-------------------+

                                  a) IPv6(A)= Prefix+encripted(E.164)
                                                    (for X packets)
                                     IPv6(A)= Prefix+encripted'(E.164)
                                                    (for Y)

                                  b) IPv6(A)=  Prefix+E.164,
                                               flowid1, (for X packets)
                                               flowid2  (for Y...)

                                  c) IPv6(A)=  Prefix+E.164,
                                               context1, (for X packets)
                                               context2  (for Y...)
```

5. DNS

    All transactions with the mobile terminal have first to go through the
DNS. It should be implemented as close to the MSC as possible. Upon
registration with the network, the CM layer has to be interfaced to the DNS
in order to update the user's IPv6 address.

   Whenever the mobile executes a handover between cells of a same MSC no
changes will be done in the DNS. However when handover are executed between
MSCs the DNS should be updated in such a way that the old entry be removed
(old Prefix) and a new entry inserted with the different Prefix (of the new
MSC).

When security is implemented with the first solution (encripted E.164), the DNS will hold the complete E.164 number of the terminal. It is not responsible of holding keys or other security informations. Those will have to be obtained by means of a dedicated protocol.

[6]. Transmission

Radio ressource is scarce and it has very specific caracteristics. In [2] guidelines to implement IP layers ontop of such medias is described. Mainly, IP header compression and the ability to manage several multiplexed channels for a single IP connection are important considerations for the implementation of SixTEL especially if voice has to be carried over IPv6 instead of the current voice channel (dedicated traffic channels).

When packets have to be sent from the mobile terminal to the network, the normal CM procedures have to be invoked to assign a channel and to update any necessary record. If the channel is already available then it should be used. Cutting off a radio channel can be done after a timeout or with an explicit signalling message. This procedure is related to the service definition in the network and is beyond the scope of this document. Finally mapping between Diff-Serv and available radio channels has to be studied.

[7]. Author's Address

Hossam Afifi, INRIA - Rodeo Project   Phone: (+33) 4 92387596
2004 route des lucioles   Fax: (+33) 4 92127030
Sophia Antipolis, 06802 France   Email:
afifi@sophia.inria.fr

Jim Bound
Member Technical Staff   Phone: (603) 881-0400
Network Operating Systems   Fax: (603) 881-0120
Compaq Computer Corporation   Email: bound@zk3.dec.com
110 Spitbrook Road, ZKO3-3/U14 Nashua, NH 03062

Scott W CADZOW Cadzow Communications Consulting Ltd. 10 Yewlands
Email: scott@cadzow.com Sawbridgeworth Herts England

Laurent Toutain   Phone: (+33) 2 99127026
ENST Bretagne   Fax: (+33) 2 99127030
2 rue de la chataigneraie   Email: toutain@rennes.enst-
bretagne.fr
Cesson Sevigne, 35512 France

8. References

1. J. Bound, B. Carpenter, D. Harrington, J. Houldsworth, A. Lloyd. OSI

NSAPs and IPv6.

    RFC-1888. (08/96).
    2. S. Dawkins, G. Montenegro, M. Kojo, V. Magret. Performance Implications of Link-Layer
       Characteristics: Slow Links. draft-ietf-pilc-slow-00.txt
    2. B. Hinden, S. Deering. IP Version 6 Addressing Architecture. Request for comments 2373. (07/98).
    3. B. Hinden, M. O'Dell, S. Deering. An IPv6 Aggregatable Global Unicast Address Format.
       Request for comments 2374. (07/98).
    4. ITU-T. E.164. The International Public Telecommunications Numbering Plan. (05/97)
    7. M. Mouly, M.B. Pautet. The GSM System for Mobile Communications. ISBN 2-9507190-0-7.
    8 Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS);
    Overall description of the GPRS radio interface; Stage 2. . TS 101 350 V6.0.1. ETSI

expires December 20th, 1999.