Routing Table Management for Mobile Router

Tim Leinmueller, Alexandru Petrescu, Christophe Janneteau, Christian Maihoefer
DaimlerChrysler AG, Telematics Research, Communication Systems,
P.O. Box 2360, 89013 Ulm, Germany
Motorola Labs, Edge Networking Research Lab (ENRL),
Parc les Algorithmes St Aubin, Gif-sur-Yvette 91193, France
{Tim.Leinmueller|Christian.Maihoefer}@DaimlerChrysler.com
{Alexandru.Petrescu|Christophe.Janneteau}@Motorola.com

***Abstract*— Mobile routers allow complete networks to be mobile. This article examines which modifications to the routing mechanism of standard IPv6 router have to be accomplished to provide network mobility as a mobile router (MR).**

A router's packet routing mechanism is controlled by entries in routing tables. Thus in case of network mobility, the natural approach consists in extending the capabilities of routing table management.

We describe limitations of standard routing table management and propose extensions for mobile networks. Our solution requires only minor changes to a normal router and provides good performance.

***Index Terms*— Mobile Router (MR), IPv6 Network Mobility (NEMO).**

I. Introduction

Transparent IPv6 network mobility is realized by the usage of at least two special nodes, a mobile router (MR) and a mobile router home agent (MRHA) [1]. These two nodes are able to provide mobility for entire networks consisting of several other nodes, not necessarily aware of mobility (see Figure 1).

The MR attaches to different access networks and communicates its current care-of address to the MRHA. The MRHA at the home link of the vehicle assures the permanent reachability of the mobile network via its home prefix. It forwards all respective packets to the MR's currently registered care-of address.

From an architectural point of view, vehicles can be looked at as ideal example of mobile networks (see [2]). The MR inside the vehicle is responsible for the connection of intra-vehicular sub-networks to different external access routers within a fixed IPv6 infrastructure, i.e. the Internet.

One can imagine the following scenario. Three persons drive in a car. Two of them use personal devices (Laptop or PDA) that are connected via Bluetooth or WLAN to the car's internal network. They use the car's uplink connection (e.g. UMTS) to be able to communicate with the Internet. At the same time, the navigation system receives updated traffic information from a traffic service station.

In contrast to mobile hosts, a mobile network as discussed in this paper allows efficient route updates only once for the entire in-vehicular network instead of an individual update for every host in the network. Furthermore, it allows that hosts participate which are not aware of mobility.

In this paper we discuss the design of a mobile router. In contrast to ordinary routers, a mobile router has to adapt its routing while it is moving. We give an overview, how a MR can achieve this routing table management and describe one approach in detail. Our approach requires only minor changes to a normal router and provides good performance.

This paper is organized as follows. In the next section we describe MR and a standard router's routing table mechanism. Then we examine the resulting problems and provide solutions, followed by the analysis of the features and the advantages of our selected solution. At the end, we provide a conclusion and an outlook on future work.

II. Background and Definitions

A. Mobile Router (MR)

MR is a combination of mobile host (described in [3]) and standard router (as described in [6]), that is capable to connect an entire mobile network to different access networks, while the mobile network does not have to change its internal network addressing scheme (i.e. the mobile network prefix [8] remains the same). The mobile network remains permanently attached to the mobile router.

A MR is configured to have one or several egress interfaces [4]. On an egress interface, MR may send router advertisements and may reply to router solicitations when MR is at home. Otherwise, when a MR

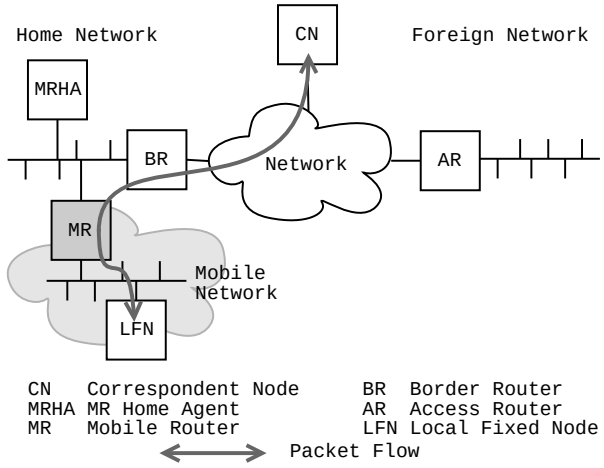

Fig. 1
MR AT HOME

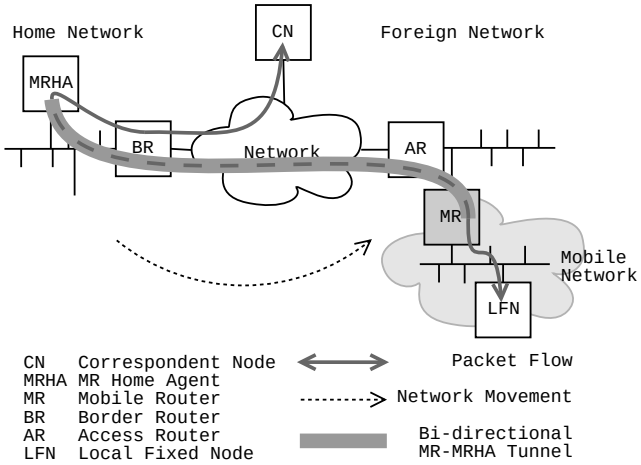

Fig. 2
MR CONNECTED TO A FOREIGN NETWORK

is not at home, it must not send router advertisements and must not reply to router solicitations on an egress interface (details on router advertisements and router solicitations can be found in [7]).

As a mobile host does, a MR detects movement by the reception of previously unknown prefixes (for further information on movement detection, see [3]). Moreover, when a MR is away from home and receives differing router advertisements, it deletes all existing entries in the Default Router List (as well as in the Neighbour Cache and in the Destination Cache).

Upon movement detection, the MR auto-configures a care-of address belonging to a prefix of the visited network. This address is then registered at a mobile router home agent in the mobile router's home network. On a change of its point of attachment, MR has to update its binding with the home agent, to point to the new care-of address.

While the mobile network is away from home, packets from and to the mobile network are always routed through the bi-directional MR - MRHA tunnel. Figure 2 shows an example communication through the tunnel between a node within a mobile network (called local fixed node in this example) and a correspondent node located somewhere in the Internet. At the home network, the border router (which interconnects the home network with the Internet) receives packets for the local fixed node. By searching in its routing table, the border router determines the MR as next hop. Since the MR is not at home, the MRHA intercepts the packets, encapsulates them and forwards them to the currently registered care-of address of the MR. At the foreign network, the access router (which offers Internet connection for mobile devices) receives the forwarded packets and delivers them to the MR. MR decapsulates the packets and delivers them to the local fixed node. The other direction, packets from the local fixed node to a correspondent node, works similar. The MR receives the packets from the local fixed node, encapsulates them and forwards them to MRHA. The MRHA decapsulates them and sends them to the border router, which delivers the packet with regular routing through the Internet. For a more detailed description of MR and MRHA, please refer to the NEMO basic support draft [1].

B. Routing Table

Routers maintain routing tables to be able to decide, how to deliver IP packets for other nodes. By comparing data from IPv6 packets (normally the destination address field) with entries in the routing table, routers try to find a suitable next hop for packets. That is either another intermediate router or the destination node itself.

A minimal routing table structure contains the following information:

- Destination IP address or destination network address.
- Destination network prefix length, 128 if the destination is a single host.
- Gateway address, that is either the host address of a router or zero. A host address requires a route to the host address or network. Zero means that the destination is located on a directly attached link.
- Destination (outgoing) network device.

Routing Table

Dest	Len	GW	Dev
3ffe:0:0:1000:::	64	fe80:2d0:59ff:fbfe:ba3	eth0
3ffe:0:0:2000:::	64	fe80:2d0:59ff:a3fe:a46	eth1
3ffe:0:0:3000:::	64	fe80:2d0:59ff:5d42:2b52	eth1

Dest Destination IP/network address
Len Destination network prefix length
GW Gateway
Dev Destination device
eth0 Mobile network ingress interface
eth1 Mobile network egress interface

Fig. 3
EXAMPLE ROUTING TABLE

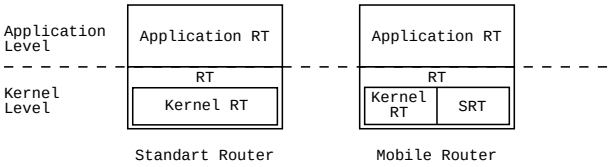

Fig. 4
ROUTING TABLE LEVELS

III. PROBLEM DESCRIPTION AND ANALYSIS

The routing table of a MR contains both, routes towards the mobile network and routes to other networks. While a MR is attached to its home link, these routes assure the functionality of the routing process and thus the connectivity of the mobile network.

As soon as a MR starts moving, i.e. attaches to a foreign link, the mobile router's routing table entries that have the egress interface as outgoing interface become invalid. In general, such entries are used to route packets that leave the mobile network, either to nodes within the MR's home network or to any other node in the Internet. While the MR is at home, these routes determine valid next-hops (routers or destination nodes), that are attached to the home link of the MR, directly addressable via an IPv6 link local address. When the MR is attached to any foreign link, these next-hops are not directly reachable any more. They cannot be reached via the link local address, since they are not on the same link. Hence, the reason for the invalidity is, that while the mobile network is not connected to its home link, all packets in direction to these routes, have to be forwarded through the MR - MRHA tunnel. On the other hand, as soon as MR returns to its home network, the routes become valid again.

To clarify this, we use the table entries as shown in figure 3. When the MR is at home, nodes in the subnet `3ffe:0:0:2000::/64` are reachable via the intermediate router `fe80:2d0:59ff:a3fe:a46`. Now when the MR is connected to a foreign link and receives packets to a node in the subnet mentioned above, MR still has the routing table entry that tells to use the next-hop `fe80:2d0:59ff:a3fe:a46`. But on the foreign link, it is likely that there is no node with such an address, and even in case there is, this must not be a router.

Therefore, the described problem has the following impact on routing table management. While being away from home, routing table management on the MR has to guarantee the modification of routing in such way that external traffic passes through the MR - MRHA tunnel. Likewise, it has to reestablish the original state of the routing table, when the mobile network returns to its home link (assuming that, while being away from home, the MR routing table has not been modified by any other process or application).

Basically, this can be achieved with the following solutions. One consists in replacing the egress interface in the respective routing table entries by a virtual device that points to the MR - MRHA tunnel. Another approach moves these routing table entries to another table and ensures that packets that leave the mobile network are sent through the tunnel. We chose the latter one since it requires only minor changes to existing architecture and thus it is simple to integrate. We suppose this solution to work together with existing routing protocol daemons and also we expect slightly better performance.

IV. SHADOW ROUTING TABLE (SRT) APPROACH

A normal router maintains different routing tables, normally at least one in kernel space and another one in user space. We call them Kernel Routing Table and Application-level Routing Table. The Kernel Routing Table is the routing table used by a router's kernel to search with for example a longest-prefix match. The Application Routing Table is used internally by a routing protocol daemon to compute shortest paths (routing daemons need separated, extended routing tables to store information related to the routing protocol, e.g. link cost). In case the computations result in modification of the Application Routing Table, the daemon reflects them to the Kernel Routing Table.

For MR we define in addition another routing table in the kernel space, the Shadow Routing Table (SRT). To keep this table invisible to normal user space applications, we also introduce an abstraction layer between Kernel Routing Table and user space, the so called Routing Table (RT). This results in the architecture as shown in figure 4. One can say, with a MR,

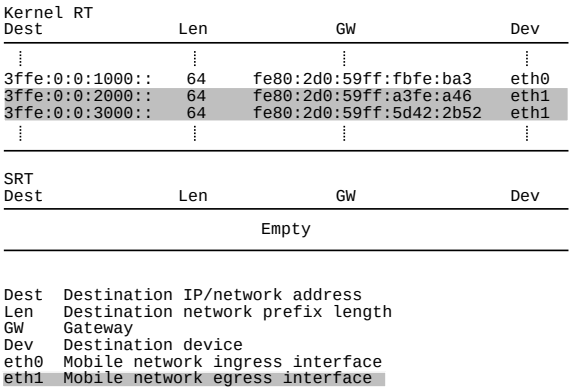

Fig. 5
ROUTING TABLES AT HOME

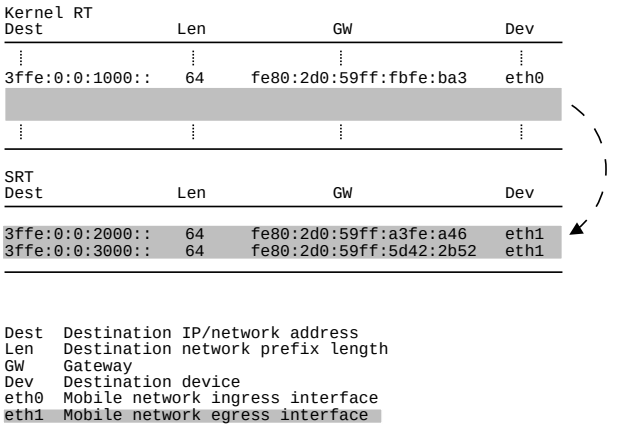

Fig. 6
ROUTING TABLES WHEN MR CONNECTED TO A FOREIGN NETWORK

the Routing Table is the sum of SRT and Kernel Routing Table, whereas with a normal router, Kernel Routing Table is the same thing as Routing Table.

The SRT is introduced to solve the routing table issue explained in the previous section. It is used by MR to temporarily store entries from the Kernel Routing Table while MR is away from home. SRT can be understood as a Binding Cache for Mobile Routers (in Mobile IPv6 [3] the mobile host does not have a Binding Cache). As soon as movement from the home network to any foreign network is detected, entries having an egress interface as outgoing interface are moved to the Shadow Routing Table. Vice versa, as soon as a movement from any foreign network to the mobile router's home network is detected, all entries from the Shadow Routing Table are moved back to the normal routing table.

A. Routing Table Management

Routing table management for MR has to accomplish the following tasks. As described in the previous section, it has to move routing table entries between SRT and the Kernel Routing Table, depending on the current location status. Figure 5 and 6 show an example. While the MR is at home (Figure 5), the SRT is empty and the Kernel Routing Table contains all routes. In figure 6, MR has moved and thus all entries containing the egress interface have been moved to SRT.

Furthermore, routing table management has to keep mobility (and thus the SRT approach) invisible from normal (i.e. mobility unaware) user space applications. This results in the behavior as described below. When a MR is connected to its home network, routing table modifications that are issued by a normal user space application are always applied to the Kernel Routing Table part of the Routing Table. Otherwise, when MR is connected to a foreign link, all additions/deletions that refer to an egress interface happen in the SRT part of the Routing Table, whereas additions/deletions that do *not* refer to such an interface are still executed on the Kernel Routing Table.

B. Dynamic Routing Protocols

Due to this management, the SRT approach is also capable to hide mobility from user space routing protocol daemons, such as RIPng [9] or OSPF [10]. At startup such a daemon copies all entries found in the Routing Table into the Application Routing Table. Additional information, e.g. about link cost and link status are received by message exchange between different routers. These information are also stored in the Application Routing Table. Subsequently, a routing protocol daemon computes new routes stores them in the Application Routing Table, and reflects the modifications to the Routing Table. The management assures that, as in the normal application case, modifications are issued in the right section of the Routing Table.

C. Destination Search Algorithm

Principally, compared to a normal router, MR uses an extended search strategy. Figure 7 shows the pseudo code implementation of the MR search algorithm. To reveal the differences, we first explain the normal router part and then we concentrate on the MR extensions.

When a normal router routes a packet, it searches its Kernel Routing Table (Figure 7, Line 01). If it

```
(01) routing table lookup(packet, in_kernel_rt):
(02) if (matching entry found) then{            Standard
(03)   send packet(packet, to_next_hop);        Router
(04) }else{
(05)   routing table lookup(packet, in_srt)
(06)   if (matching entry found) then{           Mobile
(07)     encapsulate (packet);                   Router
(08)     send packet(packet, to_HA);
(09)     }else{
(10)     send dest. unreachable (to_source);     Standard
(11)     discard (packet);                       Router
(12) }
```

Fig. 7
SEARCH ALGORITHM PSEUDO CODE

finds a corresponding destination entry, it delivers the packet (Lines 02 - 03). Otherwise, the packet is dropped (Line 04 and 11) and the router sends a destination unreachable message to the original sender (Line 10).

When MR routes a packet, as a normal router it first searches the Kernel Routing Table (Line 01). If MR finds an entry, it routes the packet normally (Lines 02 - 03). If it doesn't find an entry, then it searches the SRT (Lines 04 - 05). In case an entry is found in the SRT then that packet must be encapsulated and sent to HA through the MR - MRHA tunnel (Lines 06 - 08). If no entry is found in SRT then, as a normal router, in the end the packet is dropped and a destination unreachable message is sent (Lines 09 - 11).

D. Packet Delivery Procedure

Once a destination is found in either the Kernel Routing Table or the SRT, the MR is capable to forward the packet in direction to its destination. If the search algorithm found a next-hop in the Kernel Routing Table, then the MR forwards the packet as every other router does. It uses the outgoing interface, that is stored in the outgoing device field of the Kernel Routing Table.

In case, the destination was found in the SRT, the MR encapsulates the packet and forwards it through bi-directional MR - MRHA tunnel using the currently attached egress interface (regardless of the outgoing interface field in the SRT (see Figure 6)) to its MRHA.

E. Characteristics and Advantages

The SRT has the following characteristics. Of course, entries in the SRT are hidden from the normal packet routing algorithm, which is only executed on the Kernel Routing Table (see Figure 7).

Also, as mentioned before, the separation into separate routing tables is invisible for normal applications, that modify the routing table. Normal applications means applications, that do not support network mobility, e.g. dynamic routing protocol daemons. Modifications that are caused by such an application are automatically executed on the right table.

Furthermore, the SRT approach has no negative impact on routing performance for packets that remain in the permanently attached sub-nets, i.e. the mobile network. Local routing to the fixed networks of the MR remains unaffected. Additional delay, introduced by searching another routing table (i.e. the SRT) can be neglected, compared to the delay introduced by the MR - MRHA tunnel.

V. CONCLUSIONS

We have analysed the problem of routing table management for mobile routers and have presented a working solution, which is implemented in the Motorola LIVSIX IPv6 stack [5].

The mobile router routing table management of LIVSIX has been thoroughly tested. A LIVSIX based mobile router and the corresponding mobile router home agent are used in the IST project OverDRiVE [2] as a central component of the demonstrator.

In Future work, we will evaluate other possible solutions and compare them to Shadow Routing Table approach, especially in terms of compatibility, transparency and performance.

REFERENCES

[1] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu and Pascal Thubert, *Nemo Basic Support Protocol*, Internet Draft draft-ietf-nemo-basic-support-02.txt (Work in Progress), IETF, December 2003.

[2] OverDRiVE (Spectrum Efficient Uni- and Multicast Over Dynamic Radio Networks in Vehicular Environments), IST project IST-2001-35125

[3] David B. Johnson, Charles E. Perkins and Jari Arkko, *Mobility Support in IPv6*, Internet Draft draft-ietf-mobileip-ipv6-24.txt (Work in Progress), IETF, June 2003.

[4] Thierry Ernst, Hong-Yon Lach, *Network Mobility Support Terminology*, Internet Draft draft-ietf-nemo-terminology-00.txt (Work in Progress), IETF, May 2003.

[5] Motorola LIVSIX, an open source IPv6 stack, http://www.nal.motlabs.com/livsix/

[6] S. Deering and R. Hinden, *Internet Protocol, Version 6 (IPv6) Specification*, RFC (Standards Track) 2460, IETF, December 1998.

[7] T. Narten, E. Nordmark, and W. Simpson, *Neighbor Discovery for IP Version 6 (IPv6)*, RFC (Standards Track) 2461, IETF, December 1998.

[8] J. Manner and M. Kojo, *Mobility Related Terminology*, Internet Draft draft-ietf-seamoby-mobility-terminology-05.txt (Work in Progress), IETF, November 2003.

[9] G. Malkin and R. Minnear, *RIPng for IPv6*, RFC (Standards Track) 2080, IETF, January 1997.

[10] R. Coltun, D. Ferguson and J. Moy, *OSPF for IPv6*, RFC (Standards Track) 2740, IETF, December 1999.