Technical University Berlin

Telecommunication Networks Group

Report on CASP Mobility Client Protocol Implementation Design and First Prototype Functionality

Tianwei Chen, Sven Hermann, Günter Schäfer
[chen,hermann,schaefer]@ee.tu-berlin.de

Berlin, 06/2003

TKN Technical Report TKN-03-14

TKN Technical Reports Series

Editor: Prof. Dr.-Ing. Adam Wolisz

Abstract

This document [1] is a report on CASP mobility client protocol implementation based on the Internet Draft “QoS Resource Allocation in Mobile Networks with CASP” [4].

This document describes the design and first prototype functionalities including enhanced advertisement and CASP QoS client signaling. It also provides an initial discussion on how to optimize further the developed solutions for the seamless handovers by integrating and developing the context transfer protocol and the fast handovers for Mobile IPv6.

[1] This work has been supported by Siemens AG, ICM N PG SP RC in the context of the project “Mobility in Multi-Domain, Multi-Technology, IP-based Network” (responsible project manager: Dr. Changpeng Fan in Siemens AG, ICM N PG SP RC PN).

Contents

List of Figures

Chapter 1

Introduction

In high mobility scenarios, frequent handovers may result in a significant degradation of QoS provisioning if the access network is unable to provide enhanced solutions for prompt QoS re- establishments. Most of the current approaches for signaling protocols consider only the actions which have to be taken after a handover occurs. Some newly proposed protocols use various ideas to speed up the re-establishment of the reservation paths and handle the specific mobility related events, e.g. changes of the IP address of a mobile node. However, none of the protocols introduces mechanisms for the preparation of a handover.

Several requirements have been identified for seamless handovers and the fast re-establishment of QoS reservations:

- Bidirectional reservation. If the route is symmetric, it should be feasible to set up reservation in both directions with a single reservation message; if the route is asymmetric, a reservation message from the originator should trigger an independent signaling message from the responder.
- Path repair and re-establishment of reservations. The paths in a mobility supporting access network usually change only partially after a handover. Therefore, the protocol should support partial repairs of the paths to avoid long distance end-to-end signaling message exchanges between corresponding nodes.
- Reservation Range. The reservation range consists of a lower and an upper bound of QoS parameters e.g. bandwidth. The upper bandwidth value represents the desired bandwidth while the lower value is the acceptable bandwidth. If the network is not able to satisfy the desired value, it can reserve as much as it can if this is greater than the acceptable value. Thus, the mobile node is unnecessary to negotiate further with the network on the requested QoS as happens when only one value in a QoS request.
- Modularity. The protocol should provide a modular architecture which offers the opportunity to use different functionalities flexibly.
- Endpoint identifier. The endpoint identifier must be independent from identifiers which may change due to mobility, e.g. the IP address.

- Security model. The Security model must provide an efficient and secure solution.

All the above mentioned requirements are satisfied by the Cross Application Signaling Protocol (CASP) [10], a general-purpose protocol for managing state information in network devices.

The CASP protocol is split into two layers, a general purpose messaging layer (M-layer) and several client layers for signaling applications like QoS, MIDCOM etc. The messaging layer is used to establish session states with session identifiers. These identifiers are independent from the IP address of a node. Therefore, they can be used to identify the sessions from a mobile node easily, even after a change of the care- of address due to a handover to another access router. The CASP QoS client protocol [9] itself deals with it already. As soon as the mobile node detects a route change due to mobility (e.g. based on a layer 2 trigger), it triggers mobility related protocols. The mobility component may trigger a CASP signaling message.

In CASP, signaling and discovery message delivery are separated. The Scout protocol is used to discover the next suitable CASP node and the required soft-state refresh interval if the next CASP node is more than one network-layer hop away. It is only needed in case that no other suitable means of discovering the next CASP node are available. See [1] for reference. In environments with high mobility, however, the discovery process with scout will increase the considerable overall handover latency.

Additionally, the price information is an important criterion for the handover decision especially in heterogeneous networks.

To enable seamless QoS provisioning, we introduce the following new functionalities to address the issues mentioned above:

- Mobility supporting functions. To avoid the extra message exchanges for the discovery, each access routers broadcasts enhanced advertisements regularly, which contain the information about the next suited CASP nodes.
- QoS information before handover. The enhanced advertisements contain information about the available resources in the network and a mobile node can select the suited access router. This procedure demands an efficient and fast information distribution mechanism in the access network.
- Price information before handover. If a mobile node receives advertisements from different access networks, its decision for the next access router may depend on the price of the offered service. Therefore, the enhanced advertisements also contain an optional field for the price information.

In the following chapters, we describe the design and implementation of these functionalities to integrate the CASP QoS client protocol in the developed solutions of the SeQoMo project [1].

Chapter 2

Design of QoS Resource Allocation in Mobile Networks with CASP

This chapter first presents the message flows of the integrated SeQoMo approach with the CASP QoS client protocol in Mobile IPv6 (MIPv6) cases with or without the hierarchy support (HMIPv6). Then it discusses the design considerations of the integration.

2.1 An Overview of the Message Flows

This sections presents the message flows in HMIPv6 and MIPv6 environments separately.

2.1.1 HMIPv6

In MIPv6 with hierarchy supporting environments, the MN keeps the same CoA (i.e. RCoA) to HA and CN after intra-domain handovers. The message flow of the whole registration procedure is presented in Figure 2.1.

It is assumed that the MN has a bidirectional QoS-enabled connection with a CN before it starts an intra-domain handover. The MN receives more than one enhanced advertisements from different ARs, it can select the most suited AR as the handover target. When the handover is triggered, MN sends an re-registration request message which contains a cookie to the target AR (nAR). When nAR receives the request, it first verifies the cookie. If the verification passes, it starts the BU process. A CASP-QoS Query packet is embedded in the BU packet. Each node along the path from nAR to MAP checks whether it can satisfy at least the acceptable bandwidth for either uni-direction or bi-direction. If yes, it reserves the requested resource. When MAP (which is assumed to be the cross-over router (CR)) realizes that each node on the path can meet the request, it communicates with the AAAL for a re-authorization check. If the check passes, MAP sends back a BU ACK packet which contains a CASP-QoS Reserve message. While MAP sends the BU ACK packet, it initiates the reservation release process to tear down the path between oAR and MAP. nAR first performs a re-authentication check. If the check passes, it generates a new cookie and encrypts it with the session key which is

```
MN          oAR         nAR                     MAP(CR)     AAAL
|            |           |                        |          |
|Router Adv. |           |                        |          |
|<-----------------------|                        |          |
|            |           |                        |          |
|Registr. req. + cookie  |                        |          |
|----------------------->|                        |          |
|            |           |cookie verification     |          |
|            |           |                        |          |
|            |           |BU + CASP-QoS(Query)    |          |
|            |           |----------------------->|          |
|            |           |                        |authorization
|            |           |                        |<-------->|
|            |           |BU_ACK + CASP-QoS(Reserve)         |
|            |           |<-----------------------|          |
|            |           |authentication          |          |
|            |           |new cookie generation   |          |
|            |BU_ACK     |                        |          |
|<-----------------------|                        |          |
|            |   CASP-QoS RELEASE                 |          |
|            |<-----------------------------------|          |
```

Figure 2.1: Message Flows in HMIPv6 Intra-domain Handover Cases

included in the BU ACK message. The nAR includes the encrypted cookie in the BU ACK message and sends it to MN.

The inter-domain handover case is similar with the MIPv6 case which is discussed in the following section.

2.1.2 MIPv6

In MIPv6 handover cases or inter-domain HMIPv6 cases, a MN needs to send a BU to the HA and CN which are supposed far away from the visited access network.

Figure 2.2 shows the message flows in MIPv6 handover cases.

After the MN makes the decision to move based on the information in the enhanced advertisement, it sends a BU message to its HA. HA performs the authentication and authorization check with home AAA server. If the check passes, HA sends a BU ACK message to MN along with security asso-

```
MN          oAR         nAR         CR         HA         AAAH
|            |           |           |          |            |
|Router Adv. |           |           |          |            |
|<-----------------------|           |          |            |
|            |    Binding Update(Co oAR)        |            |
|----------------------------------------------->|AA check    |
|CASP-QoS(Query)         |           |          |<---------->|
|----------------------->|CASP-QOS(Query)       |            |
|            |           |---------->|          |            |
|            |           |           |          |            |
|            |           |CASP-QOS(Reserve)     |            |
|    CASP-QoS(Reserve)   |<----------|          |            |
|<-----------------------|           |          |            |
|            |      BU_ACK()         |          |            |
|<----------------------------------------------|            |
|            |           |           |CASP-QOS(Query)        |
|            |           |           |<---------|            |
|            |           |           |          |            |
|            |           |           | CASP-QoS(Reserve)     |
|            |           |           |--------->|            |
|            |           |           |          |            |
```

Figure 2.2: Message Flows in MIPv6 Handover Cases

ciation information e.g. session key etc. In order to minimize the registration latency, MN initiates QoS reservation process by sending a CASP-QoS Query message to CR before receiving BU ACK messages from HA. The CR makes the reservation by responding CASP-QoS Reserve message. The CR is known to MN with the help of the information in the advertisement. For example, the CR is considered as the next CASP node hence its address is presented in the advertisement. When HA acknowledges the BU, it communicates with the CR to confirm or establish the QoS path using CASP-QoS messages.

2.2 Design Considerations

The CASP-QoS messages should be included in the IPv6 hop-by-hop option header in order to enable each node long the path to check it.

An example of the CASP-QoS Query message is shown in Figure 2.3.

```
     0                   1                   2                   3
     0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
                                    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 1                                  | Option type   | Opt Data Len  |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 2  |F|D|A| Reserved|             Flow label                        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 3  |                       Lifetime                                |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 4  |                       MN Address                              |
 5  |                                                               |
 6  |                                                               |
 7  |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 8  |                Address of the next CASP node                  |
 9  |                                                               |
10  |                                                               |
11  |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
12  |                       MN-HoA*                                 |
13  |                                                               |
14  |                                                               |
15  |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
16  |                       AR Address                              |
17  |                                                               |
18  |                                                               |
19  |                                                               |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
20  |Object Type    | Object Length | desired Bandwidth             |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
21  |Object Type    | Object Length | acceptable Bandwidth          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 2.3: An Example Message Format of CASP-QoS Query Message

Chapter 3

Implementation of Enhanced Advertisements

This chapter first presents an overview of the mechanism, then introduces the existing advertisement daemon. Afterwards, it explains the design considerations. Finally, it describes the details of the implementation.

3.1 Overview of the Mechanism

Presently, the advertisement, which is sent by the access routers regularly, only includes the topology information of the access network. In MIPv6 case, mobile node can construct a new Care-of-Address (CoA) based on the advertised prefix information. Before performing a handover, mobile node may receive more than one advertisement from different access routers before the old advertisement expires.

The mechanism includes information about the available aggregated QoS of a path and about the price. A mobile node can access the most suited network which offers proper QoS and a reasonable price.

3.1.1 Message Propagation

The foreign mobility agent (e.g. MAP in HMIPv6) of a network is responsible for its own discovery. Therefore it advertises its presence downstream in the access network.

Every foreign mobility agent or intermediate router (IR) must be able to receive and propagate advertisement messages from its upstream nodes in the access network.

Figure 3.1 shows how advertisement messages propagate in a hierarchical architecture. The router in level 2 sends its advertisement to the routers in level 1, including e.g. its prefix information, the bandwidth value it can provide and the price information. The routers in level 1 receives the advertisement and extracts the useful information from it. Then it composes its own advertisement which contains

1) the prefix information of the upper router and itself; 2) QoS parameters e.g. available bandwidth of the path; and 3) the applicable price information if any. Then it sends out its advertisement. In general, the advertisements from routers in level 1 are sent more frequently than those from routers in level 2.

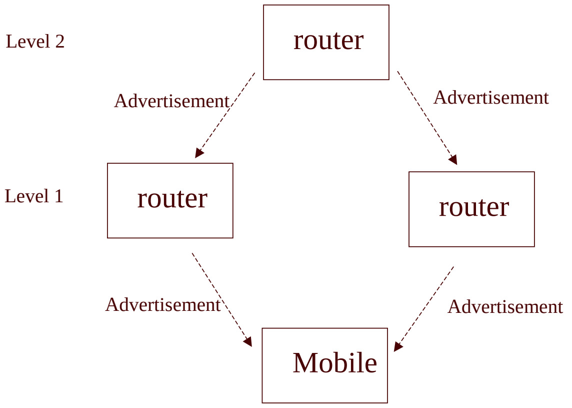


Figure 3.1: Enhanced Advertisements propagate

3.1.2 Message Format

An enhanced ICMPv6 Router Advertisement message is shown in Figure 3.2.

The details of IPv6 header and ICMPv6 router advertisement refer in [2]and [8].

We describe only the fields of the enhanced features, which are the IPv6 address of the next CASP node, available bandwidth information and a price reference label.

- Next CASP node Option:
  - Type: TBD
  - Length: 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value is 3.
  - Reserved: This field is unused.
  - Valid lifetime: This value indicates the validity duration of the announced CASP node.
  - CASP node address: The IPv6 address of "the next CASP node". This address is used as the destination address for the CASP messages which are sent by the mobile node to reserve bandwidth in the access network.
- Bandwidth and Price Information Option:
  - Type: TBD

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|vers=6 |Prio=15|               Flow Label                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |Next Header=58 | Hop Limit =255|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|      Source Address = router or home agent's address          |
+                                                               +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
| Destination Address = mobile node's address* or All-Nodes     |
+                                       multicast address      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type=134      | Code=0        |        Checksum               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Cur Hop Limit |M|O|  Reserved |       Router Lifetime         |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Reachable Time                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Retrans Timer                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type=3        | Length=4      | Prefix Length |L|A| Reserved 1|
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Valid Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Preferred Lifetime                    |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                          Reserved2                            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                (Network-)Prefix                               |
+                                                               +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                                                               :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type          | Length=3      | Reserved                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                         Valid Lifetime                        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                       CASP node address                       |
+                                                               +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
:                                                               :
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Type          |  Length=1     |Flg|       Reserved            |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
| Available Bandwidth           |  Price Reference Label        |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 3.2: Message Format of An Enhanced Advertisement

– Length: 8-bit unsigned integer. The length of the option (including the type and length fields) in units of 8 octets. The value is 1.

  - Flg: A 2-bit flag to indicate the presence of the available bandwidth and the price reference label. 11 means the advertisement contains available bandwidth and price reference label information; 10 means only available bandwidth and no price reference label; 01 means only price reference label and no available bandwidth information.
  - Available Bandwidth 16-bit unsigned integer represents the available bandwidth for each mobile node at the router.
  - Price Reference Label 16-bit unsigned integer represents the price information in the administrative domain.

More details about the mechanism are described in [4].

3.2 Introduction of the Existing Advertisement Daemon

In the current testbed, the Router Advertisement (RtAdv) daemon [3] has been extended for MAP discovery. The MAP option is attached to the RtAdv emitted by the MAP. Intermediate routers (e.g. AR) in an access network between MAP and access link are capable of receiving and propagating the received MAP options with their own RtAdvs. The RtAdv daemon has been modified to be capable of emitting its own MAP options and receiving and propagating the MAP options from other MAPs on certain links. The configuration language of radvd-0.7.1 was extended to control this behavior.

Figure 3.3 describes the behavior for MAP discovery on process level.

A router serving as MAP is responsible for initiating the MAP discovery process. Therefore, the MAP must be configurable to advertise its own MAP options and propagate MAP options from potential, topological higher MAPs along with router advertisements downstream the access network to the MN. For MAP discovery, every interface must be configurable for the following properties:

- To receive or propagate MAP options received from other interfaces.
- Whether or not its own MAP options shall be attached to an already received MAP options.
- If own MAP options are configured to be advertised, the parameters carried by the MAP option as described in the previous section.

Intermediate routers only have to receive and propagate MAP options in router advertisements. They perform essentially the same behavior for MAP discovery as the MAP itself, except that they don't emit their own MAP options. They only propagate received MAP options with router advertisements.

3.3 Design Considerations

From the topology point of view, two general cases need to be considered shown in Figure 3.4. In Case a, each AR has only one upper entity. Each AR has only one MAP option and one aggregate bandwidth information in its own RtAdv; In Case b, AR2 has two upper entities so that AR2 has one

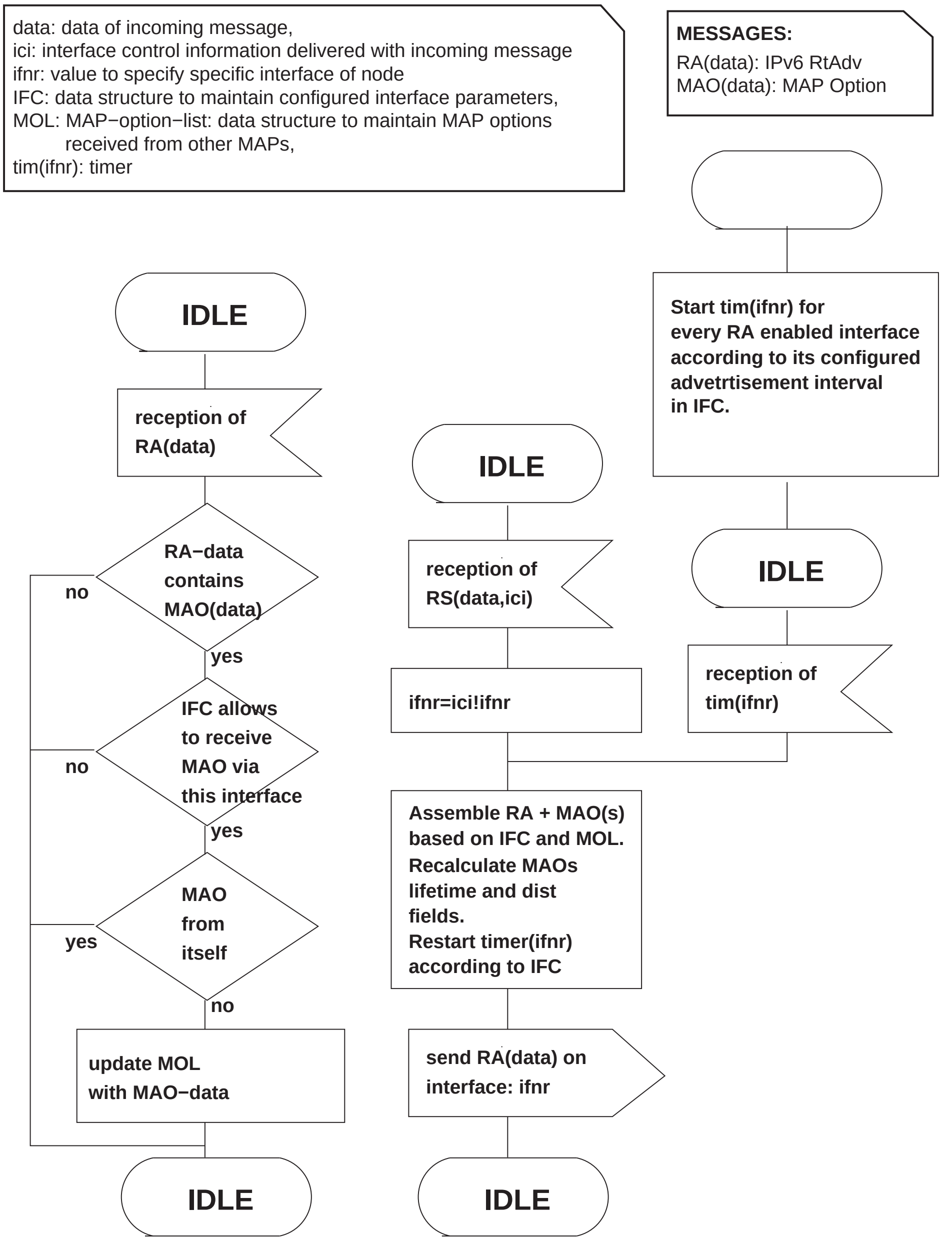

data: data of incoming message,
ici: interface control information delivered with incoming message
ifnr: value to specify specific interface of node
IFC: data structure to maintain configured interface parameters,
MOL: MAP−option−list: data structure to maintain MAP options received from other MAPs,
tim(ifnr): timer
MESSAGES:
RA(data): IPv6 RtAdv
MAO(data): MAP Option
Start tim(ifnr) for every RA enabled interface according to its configured advetrtisement interval in IFC.
IDLE
reception of RA(data)
RA−data contains MAO(data)
no
yes
IFC allows to receive MAO via this interface
no
yes
MAO from itself
yes
no
update MOL with MAO−data
IDLE
IDLE
reception of RS(data,ici)
ifnr=ici!ifnr
Assemble RA + MAO(s) based on IFC and MOL. Recalculate MAOs lifetime and dist fields. Restart timer(ifnr) according to IFC
send RA(data) on interface: ifnr
IDLE
IDLE
reception of tim(ifnr)

Figure 3.3: Pseudo-SDL description of extensions required for MAP discovery in MAP and IR

MAP option and two fields of the different aggregate bandwidth information (e.g. path via IR1 or IR2).

Two solutions can be used in the latter case:

- A branch identifier can be used to indicate which path provides which aggregate bandwidth;
- AR2 includes only the higher aggregate bandwidth value in its RtAdv immediately after the

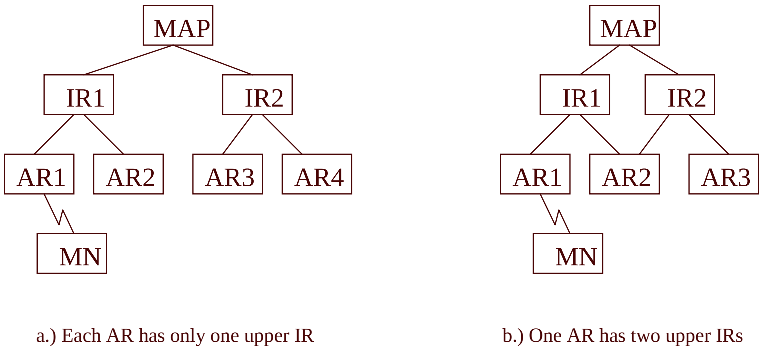

MAP
IR1
IR2
AR1
AR2
AR3
AR4
MN
a.) Each AR has only one upper IR
MAP
IR1
IR2
AR1
AR2
AR3
MN
b.) One AR has two upper IRs

Figure 3.4: Two Possible Topologies in Access Networks

MAP option. Therefore, MN can register with the MAP via AR2 to obtain the provided aggregate bandwidth. It is unnecessary for MN to know which IR its packets traverse.

To cope with the two general cases, the latter solution is implemented for the enhanced advertisement.

This solution is also true for an Mobile IPv6 network without hierarchy structure. If there is no MAP, the aggregate bandwidth information is appended along with the address field of the CASP node. The MN can send a request to the CASP node, which acts as a bandwidth broker, for the bandwidth advertisement by a specific AR.

Since we intend to show that MN selects an AR as a handover target based on new criteria: The AR which can provide the highest aggregate bandwidth is selected as the target.

In the current implementation, however, two ARs are located in one MAP domain and they use the same proc file to cache their available bandwidth. That means the two ARs always have the same available bandwidth and MN is unable to select the target AR based on the new criteria. Therefore, a modification must be made to enable the two ARs to have their independent available bandwidth. The details of the modification are described in Chapter 4.

3.4 Implementation Details

In this section, we describe the implementation details in MAP, AR and MN respectively.

In our testbed, only one-layer MAP has been implemented. The advertisement daemon at MAP, IR and AR runs in user space. The advertisement acceptance and process at MN runs in kernel.

3.4.1 MAP

MAP obtains its own bandwidth value from a proc file. Then it adds the value and price reference information in the advertisements, immediately after the MAP option. (if there is a MAP option in the RtAdv, the MAP is regarded as the next CASP node). Figure 3.5 shows the Pseudo-SDL description of the enhanced advertisement in MAP.

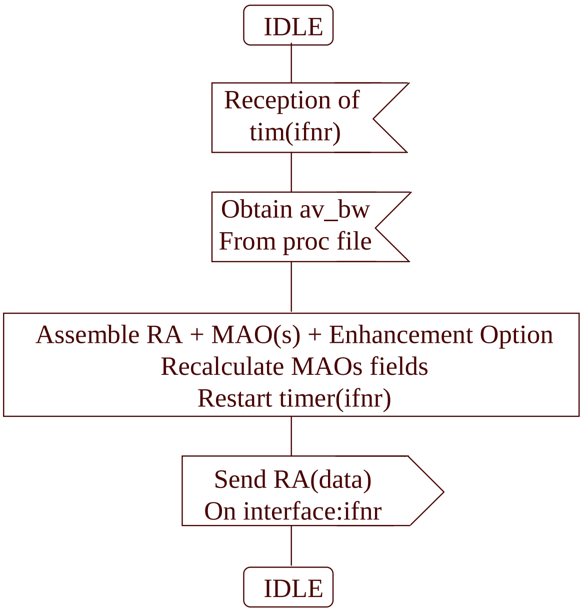

IDLE
Reception of tim(ifnr)
Obtain av_bw From proc file
Assemble RA + MAO(s) + Enhancement Option
Recalculate MAOs fields
Restart timer(ifnr)
Send RA(data) On interface:ifnr
IDLE

Figure 3.5: Pseudo-SDL description of the enhanced advertisement in MAP

The new structure for the enhancement option is shown in Figure 3.6.

Since the MAP is the first node initiating the enhanced advertisement, its other_map_list, which contains the MAP information of other MAPs, is empty.

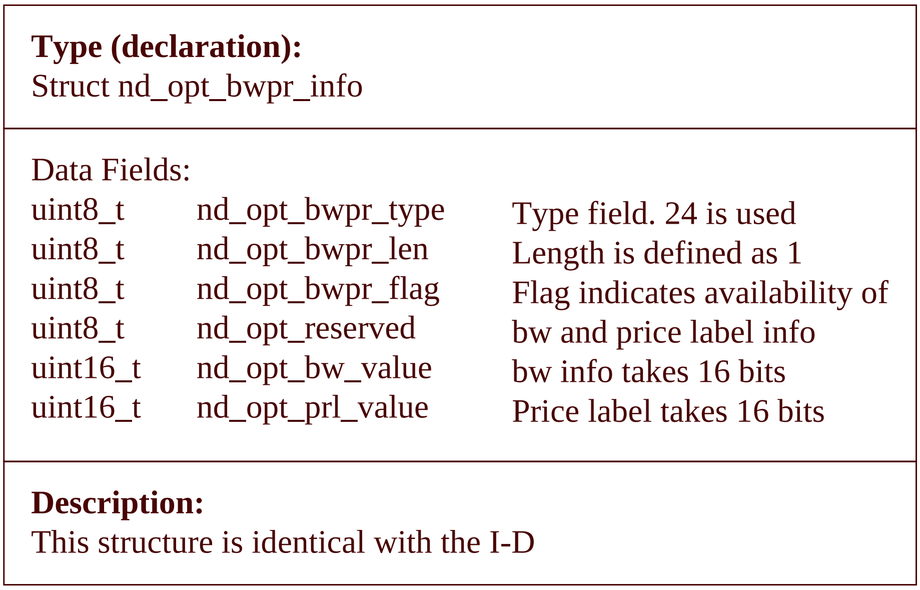
After a reservation is complete, MAP updates the av_bw in the proc file accordingly.

3.4.2 AR

The AR caches the received MAP option in its other_map_list as shown in Figure 3.3. When it is going to send out its own RtAdv, it extracts related information (including bandwidth and price) from the MAP option in the other_map_list, and puts them into its own RtAdv. Then it obtains the available bandwidth value from its proc file and compare it with the value from the MAP option. If its own value is greater, it makes no modifications to its own RtAdv. Otherwise, it replaces the bandwidth value with its own value.

Figure 3.7 shows the Pseudo-SDL description of the enhanced advertisement in AR.

After a reservation is complete, an AR updates the av_bw in the proc file accordingly.



Type (declaration):
Struct nd_opt_bwpr_info

Data Fields:

uint8_t	nd_opt_bwpr_type	Type field. 24 is used
uint8_t	nd_opt_bwpr_len	Length is defined as 1
uint8_t	nd_opt_bwpr_flag	Flag indicates availability of
uint8_t	nd_opt_reserved	bw and price label info
uint16_t	nd_opt_bw_value	bw info takes 16 bits
uint16_t	nd_opt_prl_value	Price label takes 16 bits

Description:
This structure is identical with the I-D

Figure 3.6: Data Structure of the Enhancement Option

Figure 3.8 shows the modified structure of other_map_list. One field is added in the structure to associate the enhancement option with the map option.

3.4.3 MN

The MN processes the received advertisement in kernel. Generally MN extracts the aggregate bandwidth information and makes a handover decision based on the new criteria.

Event Handling

Figure 3.9 shows an overview of MN's event handling.

ra_rcv_ptr extracts the MAP information into map_opt structure and bwpr information into bwpr_opt structure. Then h_do_map learns MAP-Infos and bwpr in the structure of "anchor". The router_event function calls router_update to update the MN's data structure.

The modification to the old MN data structure for mobility environment is shown in Figure 3.10.

The aggregate available bandwidth (aabw) information is cached with MAP parameters since the aabw is designed to be associated with the specific MAP.

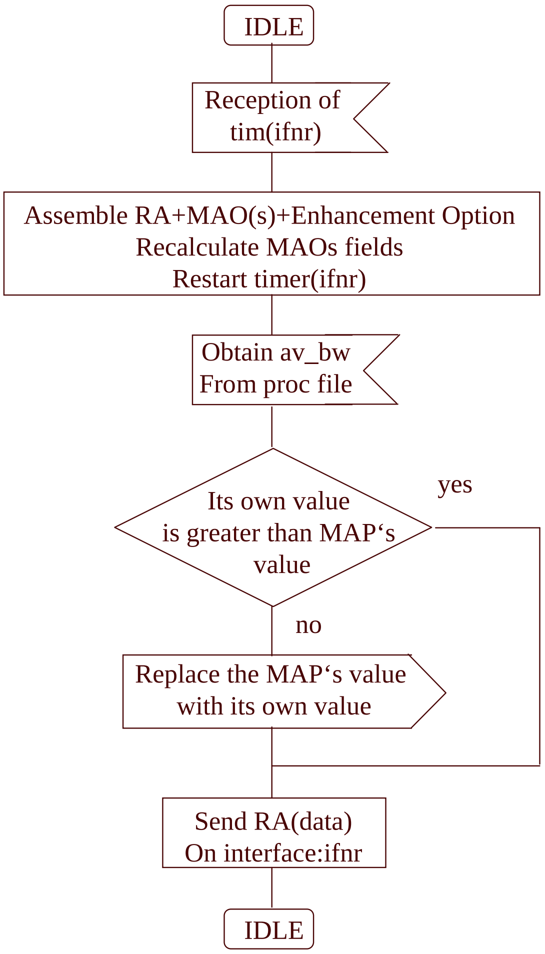

IDLE
Reception of tim(ifnr)
Assemble RA+MAO(s)+Enhancement Option
Recalculate MAOs fields
Restart timer(ifnr)
Obtain av_bw From proc file
Its own value is greater than MAP's value
yes
no
Replace the MAP's value with its own value
Send RA(data) On interface:ifnr
IDLE

Figure 3.7: Pseudo-SDL description of the enhanced advertisement in AR

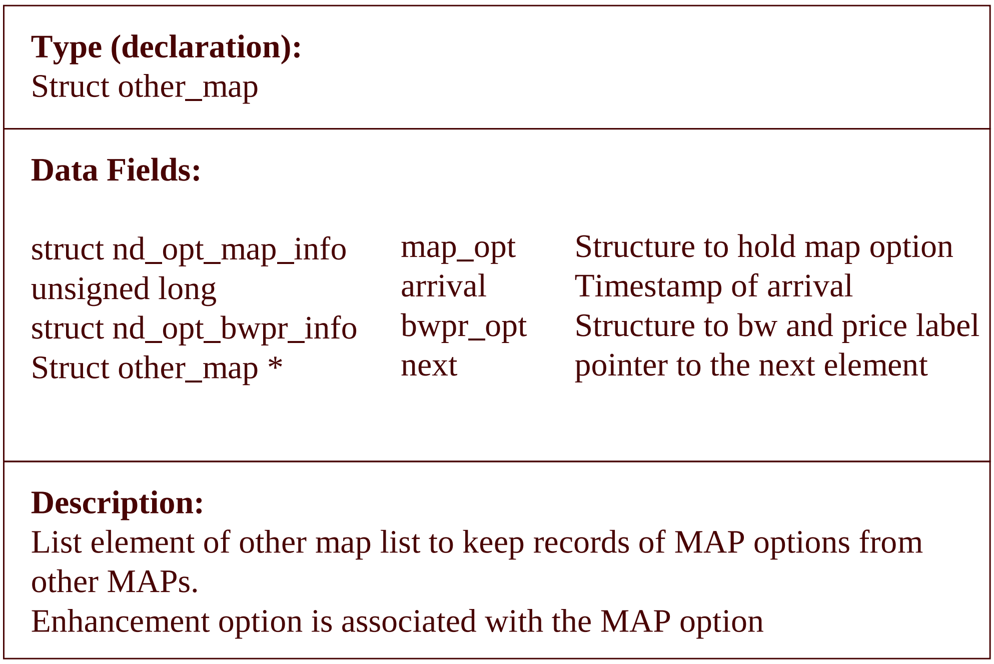
Criteria for the Handover Decision

The old criteria for the handover decision is shown in Figure 3.11. The decision is made based on the "context field". The flags are arranged in an order (depending on the policy) such that the router with the largest value in the context field is regarded as the target AR for a handover.

To take the aggregate available bandwidth information into account for the handover decision, the aabw information is designed to follow the "has MAP-Option" field. Since the aabw is 16 bits, a new data which is 32 bits (including aabw and context field) is formed for the calculation: the largest value of this data indicates the target AR.

The detailed approach is presented in Figure 3.12

The following procedure is taken to form the 32-bit data:



Type (declaration):
Struct other_map

Data Fields:

struct nd_opt_map_info	map_opt	Structure to hold map option
unsigned long	arrival	Timestamp of arrival
struct nd_opt_bwpr_info	bwpr_opt	Structure to bw and price label
Struct other_map *	next	pointer to the next element

Description:
List element of other map list to keep records of MAP options from other MAPs.
Enhancement option is associated with the MAP option

Figure 3.8: Modified Structure of Other MAP List

- context-field and 0xFC00 (take left 6 bits)
- shift to left 6 bits (right 16 bits = 0)
- sum up with 16-bit aabw (right 16 bits = aabw value)
- shift to left 10 bits (right 10 bits = 0)
- sum up with context-field's right 10 bits (i.e. context-field and 0x03FF)

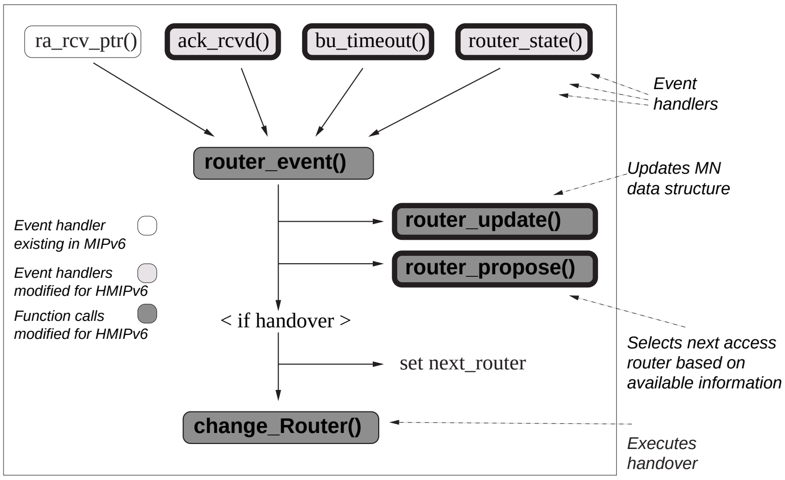

ra_rcv_ptr()
ack_rcvd()
bu_timeout()
router_state()
Event handlers
router_event()
Updates MN data structure
router_update()
router_propose()
Event handler existing in MIPv6
Event handlers modified for HMIPv6
Function calls modified for HMIPv6
< if handover >
set next_router
Selects next access router based on available information
change_Router()
Executes handover

Figure 3.9: An Overview of MN's Event Handling

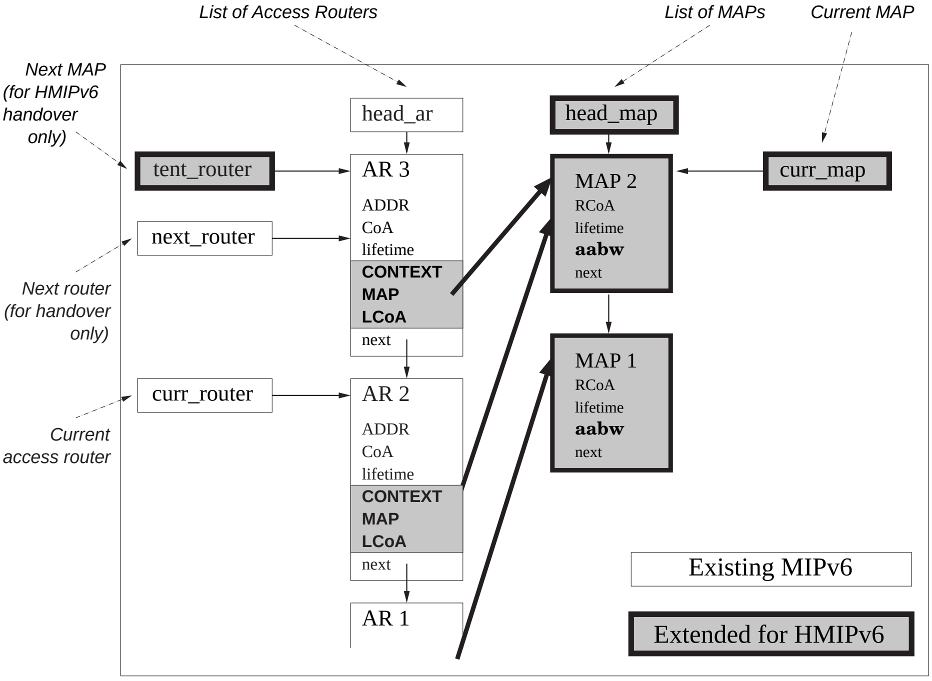


Figure 3.10: Overview of MN's Modified Data Structure for Mobility Environment

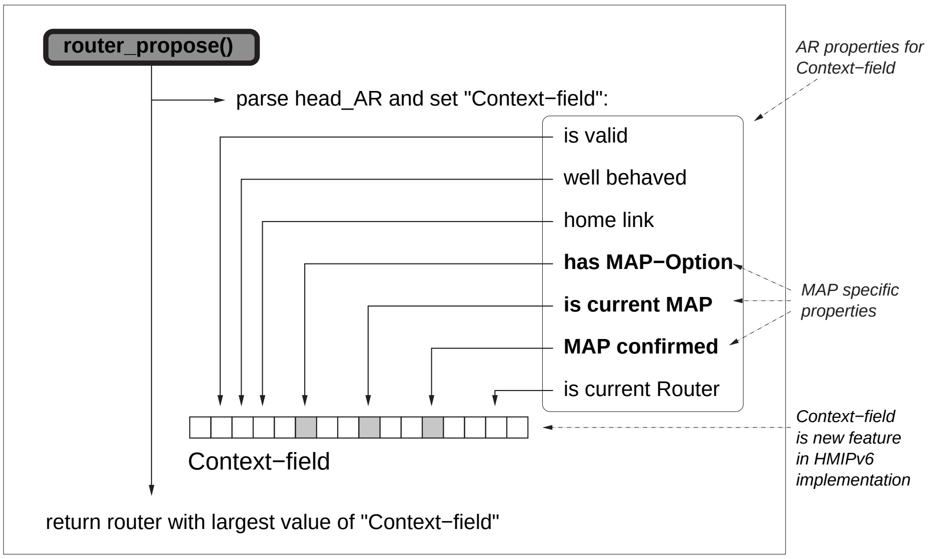

router_propose()
parse head_AR and set "Context−field":
is valid
well behaved
home link
has MAP−Option
is current MAP
MAP confirmed
is current Router
Context−field
return router with largest value of "Context−field"
AR properties for Context−field
MAP specific properties
Context−field is new feature in HMIPv6 implementation

Figure 3.11: Old Criteria for MN's Handover Decision

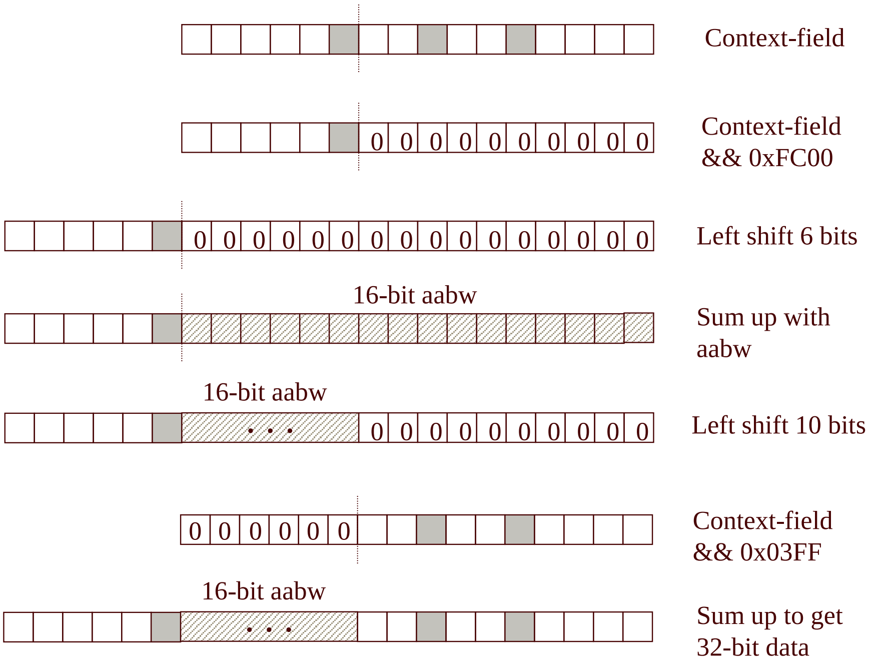


Figure 3.12: The Formation of the New Criteria for MN's Handover Decision

Chapter 4

Re-configuration of the Testbed

The mechanism for the propagation of the enhanced advertisements is based on the current implementation for MAP discovery. In the configuration of the testbed two access routers are implemented on one physical machine, the access routers ARa1 and ARa2. In the implementation both instances share the same value for the available bandwidth on the machine.

Therefore, it is necessary to split the access routers on two different machines. Figure 4.1 shows the new setup of the testbed.

The access router ARa1 is running on the former machine. The third network interface eth2 has not been removed and may be used for testing later on. During normal testing with the two separated routers it is disabled because the same IPv6 address has been assigned to the new router.

The access router ARa2 has been added to the testbed. It has the standard configuration of an AR, two physical network interfaces (eth0 and eth1) and one tunnel interface (sit2).

Additionally, the configuration of the MAP has been changed. It uses a new tunnel interface (sit5) to forward the packets to the new access router. Both access routers are logically connected to one network with the same prefix (x:x:x:2211::/64). Therefore, the prefix of the address of sit5 is the same as from sit3. The later one is the tunnel endpoint of the MAP for ARa1. The configuration files of the tunnel interfaces ifcfg-sit can be found in the file */etc/sysconfig/network-scripts/*. The configuration of the other tunnel interfaces was left unchanged. The ARb is logically located in a network with another prefix (x:x:x:2222::/64) than ARa1 and 2.

Totally, three tunnels have been installed between the MAP and the access routers. They are forwarded through the WAN emulator, which introduces WAN characteristic data traffic behaviour to the messages. In the current setup the messages are forwarded through interface eth1 of the WAM emulator. The interface eth0 is used for the traffic between the MAP and the Home Agent.

The routes from the MAP to the access routers are configured manually. They have been added to the static routes file on the affected machines. Two entries have been added for the ARa2 in the MAP, one for the tunnel interface (3ffe:b80:44c:2211::8/128) and the second for prefix of the network connected to eth1 (3ffe:b80:44c:6::/64). They were included in the file */etc/sysconfig/static-routes-ipv6* in the MAP. In the other direction, the entries for the MAP have been appended in the ARa2.

The names of the computers were assigned and registered in the */etc/hosts* file in any machine, both for the IPv4 and the IPv6 address.

All the interfaces which are connected to the physical link f need an appropriate IPv4 address because of the WAN emulator. All addresses have been chosen from the X.X.2.0/24 subnet. The IPv4 addresses are part of the configuration of the tunnel interfaces and directly included in the configuration files. Figure 4.2 shows the ifcfg-sit5 file from the MAP as an example.

The interfaces from the access routers, which are connected to the manageable hub do not need a IPv4 address for communication. Every data transfer uses version 6 of the internet protocol. The link a2 to the hub was formerly connected to ARa1 and is now attached to the new access router.

At the moment no direct connection between the access routers is required and therefore no tunnel interfaces have been installed between them.

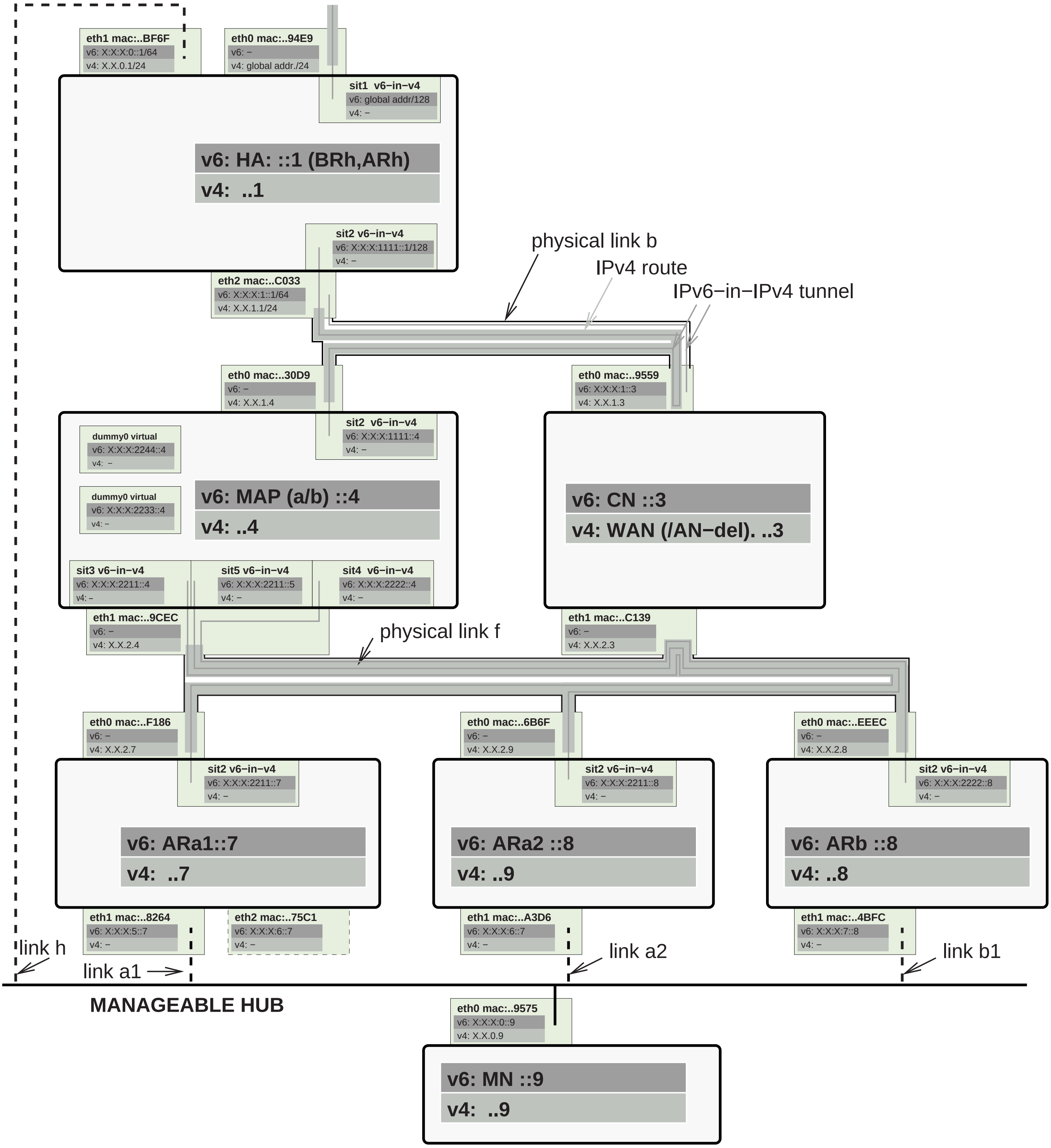


Figure 4.1: The Re-configured Testbed

```
#Example to control a dedicated IPv6-in-IPv4 tunnel interface

#       Specify interface name (must be the same as the appendix from the
filename) and other compatible values:
DEVICE="sit5"
BOOTPROTO="none"
ONBOOT="yes"

#       Control IPv6 configuration for this interface
IPV6INIT="yes" # Enable IPv6 initialization of this interface
#IPV6INIT="no" # Disable IPv6 initialization of this interface [default]

#       Specify the IPv4 address of the foreign tunnel endpoint:
IPV6TUNNELIPV4="192.168.2.9" # IPv4 address of the remote tunnel endpoint
[required]

#       Specify the IPv4 address of the local tunnel endpoint (for nodes with
more than one IPv4 address on an interface):
IPV6TUNNELIPV4LOCAL="192.168.2.4" # IPv4 address of the local tunnel endpoint
[optional]

#       Specify the local IPv6 address of a numbered IPv6-in-IPv4 tunnel
IPV6ADDR="3ffe:b80:44c:2211::5/128" # Local address of a numbered tunnel
[optional]

#       Specify the MTU of a tunnel link
#             IPV6_MTU="1280"  # set IPv6 MTU for this link [optional]
```

Figure 4.2: An Example to Control a Dedicated IPv6-in-IPv4 Tunnel Interface

Chapter 5

Discussion and Further Investigation Topics

When we recall the goal of the SeQoMo project, we can easily realize that the project mainly addresses the feature of “fast” in the mobility environments: how to minimize the latency in

- handling routing changes;
- re-establishing the QoS parameters for a flow;
- performing security checks (e.g. authentication, authorization);
- protecting QoS from DoS attacks.

The Context Transfer Protocol [7], whose key objectives are reducing latency, packet losses and avoid re-initiation of signaling to and from mobile nodes, fits in the SeQoMo project very well. Moreover, in the design of CASP and CASP-QoS Client protocols, the use of context transfer and authorization token are mentioned. But there is no detailed solution about it.

Fast Handovers for Mobile IPv6 [6], as the title suggests, aims to reduce handover latency due to IP protocol operations as small as possible in comparison to the inevitable link switching latency.

As part of the further research work, we will investigate the possibility of integrating the context transfer, fast handovers with the developed solutions. This chapter first describe the context transfer protocol and some of its open issues; then it gives a draft idea of the integration.

5.1 An Overview of the Context Transfer Protocol

"Problem Description: Reasons For Performing Context Transfers between Nodes in an IP Access Network" [5] defines the following main reasons why Context Transfer procedures may be useful in IP networks.

- The primary motivation, as mentioned in the introduction, is the need to quickly re-establish context transfer-candidate services without requiring the mobile host to explicitly perform all protocol flows for those services from scratch.
- An additional motivation is to provide an interoperable solution that works for any Layer 2 radio access technology.

Context transfer-candidate services that could utilize a context transfer solution include

- authentication, authorization and accounting;
- Quality of Service (QoS);
- header compression.

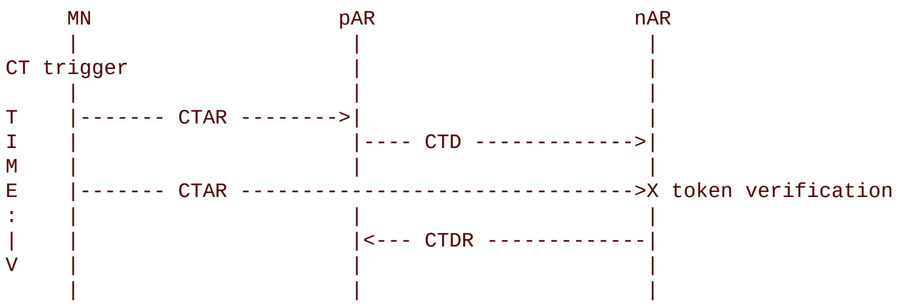
A context transfer can be either started by a request from the mobile node ("mobile controlled") or at the initiative of either the new or the previous access router ("network controlled"). The different scenarios are illustrated in the following subsections.

5.1.1 Mobile-controlled

Mobile-controlled context transfer can be further divided into two cases: MN sends a Context Transfer Activate Request (CTAR) message to the previous AR(pAR), or to the new AR(nAR).

MN first sends CTAR to pAR

Figure 5.1 shows the case that pAR transfer feature contexts when it receives a CTAR message from the MN. In this case, nAR performs the verification of the authorization token by requiring MN to present its authorization token or receiving the authorization token in MN’s CTAR.



```
     MN                    pAR                    nAR
     |                      |                      |
CT trigger                  |                      |
     |                      |                      |
T    |------- CTAR -------->|                      |
I    |                      |---- CTD ------------->|
M    |                      |                      |
E    |------- CTAR ------------------------------->X token verification
:    |                      |                      |
|    |                      |<--- CTDR -------------|
V    |                      |                      |
     |                      |                      |
```

Figure 5.1: pAR transfer feature contexts when it receives a CTAR message from the MN

CTAR contains the information of

- MN’s previous IP address;
- nAR’s IP address;
- feature contexts to be transferred;
- a token authorizing the transfer.

CTD contains the information of

- MN’s previous IP address;
- nAR’s IP address if known;
- the parameters for nAR to compute an authorization token

CTAR sent from MN to nAR may be required by nAR. CTDR reports to pAR the status of processing the received contexts.

Performing context transfer before the MN attaches to nAR has potential benefit clearly for the better performance. For this to take place, certain conditions must be met. For example, pAR must have sufficient time and knowledge about the impending handover. This is feasible for instance in Mobile IP fast handovers.

MN first sends CTAR to nAR

Figure 5.2 shows the case that nAR sends a CT Request to pAR when it receives a CTAR message from the MN. In this case, pAR performs the verification of the authorization token. It is supposed that pAR already knows the parameters for the verification.

CT Request contains the information of

- MN’s previous IP address;
- feature contexts to be transferred;
- an authorization token generated by MN.

CTD contains the information of

- MN’s previous IP address;
- feature contexts.

This case happens when the advance knowledge of impending handover is not available, or if a mechanism such as fast handover fails. Retrieving feature contexts after the MN attaches to nAR is the only available means for context transfer. Performing context transfer after handover might still be better than having to re-establish all the contexts from scratch.

```
      MN                    pAR                      nAR
      |                       |                       |
new L2 link up                |                       |
      |                       |                       |
 CT trigger                   |                       |
      |                       |                       |
 T    |------- CTAR --------------------------------->|
 I    |                       |                       |
 M    |                       X<--- CT Request -------|
 E    |   token verification/|                       |
 :    |                       |--------- CTD -------->|
 |    |                       |                       |
 V    |                       |<-------- CTDR --------|
      |                       |                       |
      |                       |                       |
```

Figure 5.2: nAR sends a CT Request to pAR when it receives a CTAR message from the MN

Additionally, some contexts may simply need to be transferred during handover signaling. For instance, any context that gets updated on a per-packet basis must clearly be transferred only after packet forwarding to the MN on its previous link is terminated. Transfer of such contexts must be properly synchronized with appropriate handover messages, such as Mobile IP (Fast) Binding Update.

5.1.2 Network-controlled

Figure 5.3 and 5.4 shows the signaling flows of CT initiated by pAR and by nAR respectively.

```
     MN                     pAR                     nAR
     |                       |                       |
     |                  CT trigger                   |
T    |                       |                       |
I    |                       |---- CTD ------------->|
M    |                       |                       |
E    |------- CTAR --------------------------------->X token verification
:    |                       |                       |
|    |                       |<--- CTDR -------------|
V    |                       |                       |
     |                       |                       |
```

Figure 5.3: CT is initiated by pAR

Context Transfer takes place when an event, such as a handover, takes place. We call such an event a

```
     MN                    pAR                     nAR
     |                      |                       |
T    |                      |                  CT Trigger
I    |                      |                       |
M    |                      X<--- CT Request -------|
E    |   token verification/|                       |
:    |                      |--------- CTD -------->|
|    |                      |                       |
V    |                      |<-------- CTDR --------|
     |                      |                       |
     |                      |                       |
```

Figure 5.4: CT is initiated by nAR

Context Transfer Trigger. In response to such a trigger, the pAR may transfer the contexts; the nAR may request contexts; and the MN may send a message to the routers to transfer contexts. Such a trigger must be capable of providing the necessary information, such as the MN's IP address with which the contexts are associated, the IP addresses of the access routers, and authorization to transfer context.

In both cases, it is supposed that pAR has the knowledge of the parameters for verifying the MN's authorization token. It sends the information to nAR in the Context Transfer Data message (CTD) so that nAR can perform the verification of the authorization token when it receives CTAR from MN.

MN sends CTAR to nAR independently in time from the rest of signaling flows.

5.1.3 Open Issues

In addition to the issue of "Failure Handling" in [7], some issues are identified as follows:

- Security Association (SA) between ARs in advance. In order to secure (i.e. for authentication, message integrity and confidentiality purposes) the context transfer signaling flows, an SA between the communicating ARs is demanded. However, sometimes it is not true to assume a SA has been pre-established between ARs, especially when context transfer signaling is not restricted only within a single domain.

- Authentication and authorization of MN. Either one or both of the pAR and nAR need to be able to authenticate the mobile and authorize mobile's credential before authorizing the context transfer and release of context to the mobile. In case the context transfer is request by the MN, a mechanism must be provided so that requests are authenticated (regardless of the security of context transfer itself) to prevent the possibility of launching DoS attacks by sending large number of CT requests as well as cause large number of context transfers between ARs [7].

- Another important consideration is that the mobile node should claim it's own context, and not some other masquerader. One method to achieve this is to provide an authentication cookie to be included with the context transfer message sent from the pAR to the nAR and confirmed by the mobile node at the nAR [7].

5.2 An Overview of Fast Handovers for MIPv6 (FMIPv6)

The overall handover protocol is illustrated in Figure 5.5 [6].

```
   MN                    pAR                  nAR
    |                     |                    |
    |------RtSolPr------->|                    |
    |<-----PrRtAdv--------|                    |
    |                     |                    |
    |------F-BU---------->|--------HI--------->|
    |                     |<------HACK---------|
    |          <--F-BACK--|--F-BACK-->         |
    |                     |                    |
 Disconnect               |                    |
    |                   forward                |
    |                   packets===============>|
    |                     |                    |
    |                     |                    |
Connect                   |                    |
    |                     |                    |
    RS (with FNA option)======================>|
    |<-----------RA (with NAACK option)--------|
    |<=================================== deliver packets
    |                                          |
```

Figure 5.5: Fast Handover Protocol Messages

There are three phases in the protocol operation: handover initiation, tunnel establishment and packet forwarding on the established tunnel.

5.2.1 Handover Initiation

The RtSolPr message allows a MN to request the IP address, link-layer address as well as network prefix of the nAR's interface to which the MN may attach to. In a network-controlled handover, the PAR supplies this information without the MN requesting it.

It is possible that the pAR itself may initiate handover by gratuitously sending a PrRtAdv message.

When the pAR sends such a message without the MN sending a RtSolPr message first, the MN MUST be prepared to process PrRtAdv message, and send an Fast Binding Update message in response.

When there is no anticipating a handover as described above, the interface between the link-layer handover mechanism and IP stack may not be well-defined or is available. In such cases, the MN may change its link without engaging in protocol messages with the pAR on its previous link. The MN should send a Fast Binding Update to the pAR as soon as it establishes connectivity with the nAR. This FBU message serves to establish a tunnel between the access routers.

5.2.2 Tunnel Establishment

Since the MN cannot use NCoA until it completes Binding Update with its Home Agent and the correspondents, it is allowed to use PCoA until it establishes itself as a Mobile IPv6 end-point. For this purpose, the nAR tunnels packets sent with PCoA as source IP address to the pAR. And, until the correspondent nodes establish a binding cache entry for NCoA, they continue to send packets to PCoA, which need to be forwarded to the MN. The pAR tunnels these packets to the nAR, which then forwards them using a host route entry to the MN. Since it is desirable to deliver these packets independent of NCoA configuration, the pAR tunnels packets to the nAR instead of to the NCoA. However, the MN MAY include NCoA as the target address for the tunnel.

The tunnel establishment is achieved through Handover Initiate (HI) and Handover Acknowledge (HAck) messages.

5.2.3 Packet Forwarding

The MN sends a Fast Binding Update (FBU) message preferably prior to disconnecting its link. When the pAR receives an FBU, it waits until the requested handover is accepted by the nAR as indicated in the HACK message status code. Then, it verifies that the source IP address in FBU is PCoA for which pAR has forwarded packets previously. And, it creates a tunnel for forwarding packets meant for PCoA to nAR. Finally, it sends a Fast Binding Acknowledgment (FBACK) message to the MN. This message is sent on the old link as well.

As soon as the MN establishes link connectivity with the nAR, it sends a Fast Neighbor Advertisement (FNA) message, which is encoded as an option in the Router Solicitation message. Only after it receives a confirmation to use NCoA in a Router Advertisement with Neighbor Advertisement Acknowledge (NAACK) option, the MN uses NCoA. If the MN has already received confirmation to use NCoA via FBACK, it includes the FNA option anyway to announce its presence to the nAR.

5.3 A Draft Proposal

Based on the proposal of the integration of CT and FMIPv6 in [11], a draft proposal to solve the identified issues in CT and integrate CT and FMIPv6 is presented as shown in Figure 5.6.

Before MN initiates a handover procedure, it is assumed that MN has a SA with pAR sharing a session key and MN is granted a colored cookie, which contains its authorization information.

```
              MN                    pAR                  nAR
               |                     |                    |
               |<==SA(SessionKey)===>|                    |
               |                     |                    |
Phase 1.       |------RtSolPr------->|                    |
               |<-----PrRtAdv--------|                    |
               |<--------RtAdv(enhanced)------------------|
               |                     |                    |
Phase 2.       |CTAR+colored cookie->|                    |
               |                     Xcookie verification |
               |                     |------CTD(HI)------>|
               |                     |                    |
Phase 3.       |--CTAR+colored cookie-------------------->|
               |                     |                    X cookie and token
               |                     |<---CTDR(HACK)------|verifications
               |<=========SA(SessionKey)=================>|
               |                     |                    |
Phase 4.    Disconnect               |                    |
               |                   forward                |
               |                   packets===============>|
               |                     |                    |
               |                     |                    X BU and QoS establishment
               |                     |                    |processes (e.g. CASP-QoS
               |                     |                    | client or RSVP)
               |                     |                    |
Phase 5.   Connect<-----acknowledge nCoA------------------|
               |                     |                    |
               |<=================================== deliver packets
               |                                          |
```

Figure 5.6: A Draft Proposal As the Further Investigation

- Phase 1. MN sends RtSolPr message as in FMIPv6 or it receives an enhanced advertisement from nAR. It makes a handover decision based on the information in the enhanced advertisement.

- Phase 2. MN sends a message to pAR including CTAR and the colored cookie which is encrypted with the session key. pAR verifies the colored cookie. If the verification passes, pAR authenticates MN and authorizes the MN's QoS request successfully. Then it sends CTD to nAR. This message can be regarded as HI as in FMIPv6. The CTD contains the parameters for nAR to verify the colored cookie and the authorization token, including the session key etc.

- Phase 3. MN sends a message to nAR also including CTAR and the colored cookie which is transmitted in plain text. nAR verifies both the colored cookie and authorization token. If the verifications are successfully, nAR assures that MN claims its own context. Then nAR sends a CTDR, which is regarded as HACK in FMIPv6, to pAR. So far, nAR and MN has set up a SA also by sharing the session key.

- Phase 4. Even though MN has to disconnect pAR, pAR forwards packets to nAR to avoid a great degree of packet loss. Then nAR initiates the BU and QoS establishment processes by means of e.g. CASP-QoS client or RSVP protocol.

- Phase 5. When the processes succeed, nAR acknowledges MN to use the nCoA and grants MN a new colored cookie. nAR starts to deliver packets to MN.

Chapter 6

Conclusions and Future Work

In this report, we described the CASP mobility client protocol implementation especially the enhanced advertisement, the design of QoS Resource Allocation in Mobile Networks with CASP.

The enhanced advertisements of access routers which include additional information such as currently available bandwidth and price can help a mobile node to select the most suited access router as the handover target.

The design and implementation of integrating CASP into the SeQoMo architecture is under progress, targeting on joining the features of CASP with the developed concepts in SeQoMo especially the "fast" feature regarding re-establishment of QoS and security states.

To achieve the overall optimized performance in a handover procedure shown as in Figure 6.1, the potential latency at every element in the generic handover model should be evaluated and minimized; and interactions of different operations should be considered.

The overall performance in terms of low registration latency in the generic handover procedure should be optimized. However, current solutions are motivated only to one specific aspect or some of them. For example, micro-mobility management protocols, multicast approaches, the fast handover scheme etc. aim only to achieve a seamless handover procedure in the aspect of mobility management; The integration of Mobile IP and AAA provides neither fast handover support nor QoS set up; The effort on light-weighted signaling design are motivated partly to provide QoS establishment in mobility scenarios; Context transfer claims to re-establish AAA (authentication, authorization and accounting) and QoS during a handover. But the demanded assumption of the pre-existing security association between two adjacent access routers or servers is not practical sometimes. Moreover, there is no sophisticated proposal on context transfer yet.

To investigate further on a efficient and secure handover procedure, CT and FMIPv6 is being considered to be integrated in the SeQoMo architecture due to the following reasons:

- the intention of CT is to reduce latency, packet losses and avoid re-initiation of signaling to and from mobile nodes;
- FMIPv6 aims to reduce handover latency due to IP protocol operations as small as possible in comparison to the inevitable link switching latency.

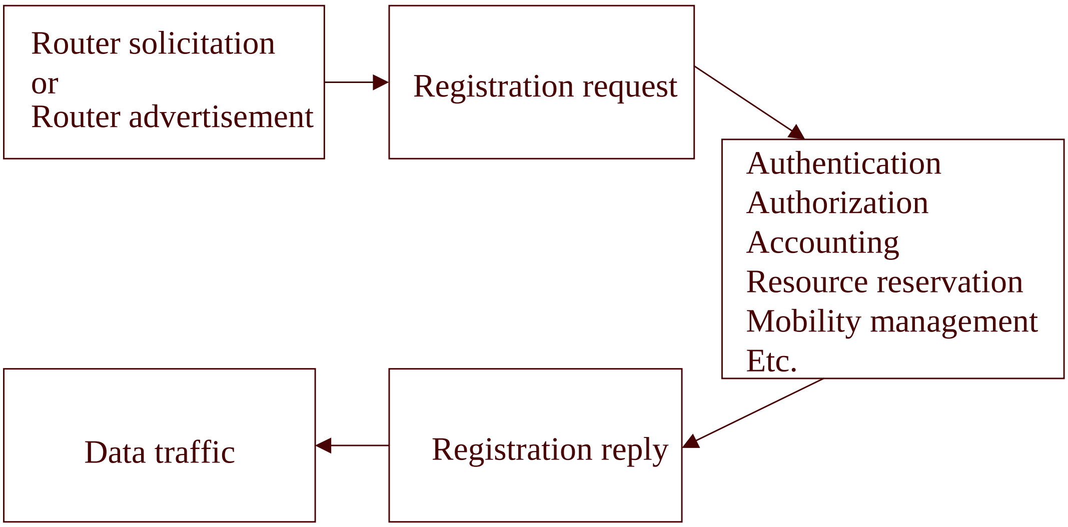


Figure 6.1: A Generic Handover Procedure Model

- CT and authorization token are two key concepts in CASP and CASP-QoS client protocol designs, which can be beneficial in the SeQoMo architecture.

Moreover, MN should be able to authenticate the source of an advertisement, and to check the integrity of QoS and price information in an advertisement. If a malicious node modifies the price distribution information or it advertises wrong information masquerading a legal AR, it can cause trouble or confusion to mobile users or to the service provider when mobile nodes do not perform the security checks.

The future work is to finish the implementation of the integration of SeQoMo and CASP concepts, work out a scheme to secure the enhanced advertisements, integrate the concepts of CT, authorization token, FMIPv6 into the current conclusive results in the SeQoMo project.

Chapter 7

Acronyms

AA Authentication and Authorization

AAA Authentication, Authorization, Accounting

AAAL local AAA server

AAAH home AAA server

aabw aggregate available bandwidth

ACK Acknowledgement

AR Access Router

BA Binding Acknowledgement

BU Binding Update

CASP Cross Application Signaling Protocol

CN Corresponding Node

CoA Care-of Address

CR Corss-over Router

CT Context Transfer

CTAR Context Transfer Activate Request

CTD Context Transfer Data

CTDR Context Transfer Data Reply

CTP Context Transfer Protocol

CT Request Context Transfer Request

DoS Denial of Service

FBACK Fast Binding Acknowledgment

FBU Fast Binding Update

FMIP Fast Handovers for MIPv6

FNA Fast Neighbor Advertisement

FPT Feature Profile Types

HA Home Agent

HI Handover Initiate

HACK Handover Acknowledge

HMIP Hierarchical MIP

HMIPv6 Hierarchical Mobile IPv6

HO Handover

HoA Home Address

HOA HOme-agent-Answer

ICMP Internet Control Message Protocol

ICMPv6 Internet Control Message Protocol version 6

ID identification

I-D Internet Draft

IETF Internet Engineering Task Force

ifnr value to specify specific interface of node

IP Internet Protocol

IPv6 Internet Protocol version 6

IR Intermediate Router

L2 layer-2

LXR Linux Cross Reference

MAC Medium Access Control

MAP Mobile Anchor Point

MIDCOM Middlebox Communication

MIP Mobile IP

MIPL Mobile IP for Linux

MIPv6 Mobile IPv6

MN Mobile Node

nAR New Access Router

NbAdv Neighbor Advertisement

NCoA New CoA

NSIS Next Steps in Signaling

pAR Previous Access Router

PCoA Previous CoA

PrRtAdv Proxy Router Advertisement

QoS Quality of Service

RA Router Advertisement

radvd router advertisement daemon

RFC Request For Comment

RS Router Solicitation

RtAdv Router Advertisement

RtSol Router Solicitation

RtSolPr Router Solicitation for Proxy

RSVP Resource Reservation Protocol

SA Security Association

SDL Specification and Description Language

TBD To Be Determined

tim(ifnr) timer

Bibliography

[1] T. Chen, A. Festag, A. Neumann, S. Hermann, X. Fu, H. Karl, and G. Schäfer. SeQoMo: Secure, QoS-Enabled Mobility Support for IP-Based Networks, March 2003.

[2] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification, December 1998.

[3] GO/Core project at HUT Telecommunication and Multimedia Lab. Mobile IP for Linux (MIPL) mipv6-0.9-v2.4.7.

[4] S. Hermann, T. Chen, G. Schäfer, and Changpeng Fan. QoS Resource Allocation in Mobile Networks with CASP, June 2003.

[5] J. Kempf. Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network, September 2002.

[6] R. Koodli(ed.). Fast Handovers for Mobile IPv6. INTERNET DRAFT draft-ietf-mobileip-fast-mipv6-06.txt, March 2003.

[7] J. Loughney, M. Nakhjiri, and C. Perkins. Context Transfer Protocol, June 2003.

[8] T. Narten, E. Nordmark, and W. Simpson. Neighbor Discovery for IP Version 6 (IPv6), December 1998.

[9] H. Schulzrinne, H. Tschofenig, X. Fu, and J. Eisl. A Quality-of-Service Resource Allocation Client for CASP, March 2003.

[10] H. Schulzrinne, H. Tschofenig, X. Fu, and A. McDonald. Cross-Application Signaling Protocol, March 2003.

[11] M. Thomas. Analysis of Mobile IP and RSVP Interactions, October 2002.