IETF Seamoby Working Group
INTERNET-DRAFT
16 October 2002

Govind Krishnamurthi,
Editor,
Nokia Research Center

Requirements for CAR Discovery Protocols

draft-ietf-seamoby-card-requirements-02.txt

Status of This Memo

Copyright Notice

ABSTRACT

The pre-requisite for IP based seamless mobility protocols is the knowledge of the access router (AR) to which a mobile node can be handed over to. Further, a handoff can be optimized if the capabilities of the AR being considered for handoff are known. The protocol which discovers ARs for potential handoff along with their capabilities is called the CAR discovery protocol. In this draft we list the requirements which are to be met by any solution for CAR Discovery.

TABLE OF CONTENTS

1. INTRODUCTION

CAR discovery protocols perform the function of identifying the candidate access routers along with their capabilities for a mobile node's (MN) handoff. CAR discovery can be used by seamless handoff protocols [1,2,3,4] to decide the access router to which the mobile node will be handed over to. The problem statement for CAR discovery is discussed in [5]. In this draft, we present the requirements that any solution for CAR discovery needs to satisfy.

2. TERMINOLOGY

In this draft, we use the same terminology as described in [5].

Access Point (AP)

A radio transceiver by which an MN obtains Layer 2 connectivity with the wired network.

Access Router (AR)

An IP router residing in an access network and connected to one or more APs. An AR offers IP connectivity to MN.

Capability of AR

A characteristic of the service offered by an AR that may be of interest to an MN when the AR is being considered as a handoff candidate.

Candidate AR (CAR)

An AR to which an MN has a choice of performing IP-level handoff. This implies that the MN has the right radio interface to connect to an AP that is served by this AR, as well as the coverage of this AR overlaps with that of the AR to which the MN is currently attached to.

Target AR (TAR)

An AR with which the procedures for the MN's IP-level handoff are initiated. TAR is selected after running a TAR Selection Algorithm that takes into account the capabilities of CARs, preferences of the MN and any other local policies.

3. REQUIREMENTS FOR THE CAR DISCOVERY SOLUTION

In this section, we list the set of requirements that must be met by the CAR discovery solution. Generic IETF practices such as re-use of existing IETF protocols wherever possible MUST be adhered to when designing the CAR discovery solution.

3.1 IDENTIFYING THE IP ADDRESS OF A CAR

If an AP identifier is forwarded as an input to the CAR discovery protocol it MUST be able to map the identifier to the IP address of the AR which the AP is connected to. This is motivated by the fact that, for example, an MN may only be able to receive the link layer identifier of an AP connected to potential target ARs. This has to be mapped to the IP address of the AR the AP is connected to. The exact identifiers that are advertised for different link layer technologies can be obtained from the appropriate standards. However, in some cases, the CAR discovery solution may be able to directly identify the IP address of the CAR. In such a case, the previously mentioned mapping from the L2 identifiers to IP addresses of ARs may not be necessary.

3.2 SUPPORT FOR INTER-TECHNOLOGY HANDOFFS

Though not common now, it is possible that in the future, MNs may have interfaces belonging to different technologies thus facilitating the possibility of inter-technology handoffs. An example for this, among others, is a handoff from an 802.11 based LAN to a 3G based cellular network. The CAR discovery solution therefore MUST be able to identify the IP addresses of CARs connected to APs of a different technology.

3.3 IDENTIFYING CARS HAVING SITE-LOCAL AND PRIVATE ADDRESSES

Support for handoffs between IPv4 and IPv6 is critical in the design of protocols dealing with mobility. Once IPv4 networks come into the picture we have to deal with the possibility of private address spaces. Even in the case of IPv6 networks, we have the possibility of private spaces. For example, the policy of a particular domain may be not to expose the globally routable IPv6 addresses of its ARs for security reasons. To support such scenarios, the CAR discovery solution MUST be able to discover CARs with non globally routeable IP addresses along with their capabilities. This is contingent on whether the operator of the network permits such handoffs.

3.4 CAPABILITY DISCOVERY

The CAR discovery solution MUST provide functionality to discover a CAR's capabilities. The CAR discovery solution MUST be able to provide the MN with CAR information. The CAR discovery solution MUST NOT be designed as a generic service discovery protocol.

3.5 UTILIZATION OF NETWORK RESOURCES FOR CAR DISCOVERY

The CAR discovery solution MUST be able to make efficient use of the network resources and SHOULD avoid the transmission of unnecessary information to the MN.

3.6 FORMAT OF CAPABILITIES

This is a requirement for inter-operability. The capabilities of CARs MUST be described in a standard format. The format is TBD.

3.7 SCOPE OF CAR DISCOVERY

The Internet is formed by several administrative domains clustered together. As explained in [5], CARs could belong to different administrative domains separated by large distances in terms of IP hops. Therefore, the CAR discovery solution MUST have an Intra-domain scope and SHOULD have Inter-domain scope.

3.8 INTRODUCTION OF DEDICATED NETWORK ELEMENTS FOR CAR DISCOVERY

The CAR discovery solution MUST NOT introduce network elements dedicated to CAR discovery.

3.9 INVOLVEMENT OF NON-CARs IN CAR DISCOVERY

Handoffs might happen very frequently. If the CAR discovery process introduced additional load on ARs which are not CARs, this will impede their performance. Therefore the CAR discovery solution SHOULD minimize the involvement of non-CARs.

3.10 DEPENDENCE ON A MOBILITY MANAGEMENT PROTOCOL

CAR discovery MUST NOT depend on a particular mobility management protocol. In other words, it MUST NOT depend on a feature which is unique to a particular mobility management protocol. The output of CAR discovery, however, MUST be usable by mobility management protocols. CAR discovery MUST NOT deteriorate the performance of the underlying mobility management protocol.

3.11 EFFECT OF CHANGES IN NETWORK TOPOLOGY

Networks topology can change for several reasons, for example, network renumbering. The CAR discovery solution MUST be adaptive to such changes in the topology of the network.

3.12 PROVIDING THE MN's REQUIREMENTS TO THE CAR DISCOVERY SOLUTION

The CAR discovery solution MUST provide means for the MN to provide its requirements. These requirements MUST be used in determining the CARs for the MN. The MN preference solution SHOULD be logically separate from the CAR information distribution solution in order to maintain separation of security requirements.This requirement is needed in the case when the CAR discovery solution needs to transfer an MN's preferences to the TAR selection algorithm.

3.13 SECURITY REQUIREMENTS

3.13.1 SECURE CAPABILITY TRANSFER

The CAR discovery solution MUST ensure that the capability information of CARs is transferred in a secure fashion. The CAR discovery solution MUST be able to authenticate and SHOULD be able to encrypt the capability information being transferred between network entities and between network entities and the MN.

3.13.2 VERIFICATION OF ROUTER AUTHENTICITY

This requirement has the following parts:
(i) The CAR discovery solution MUST be able to verify that the router under consideration as a CAR is a genuine AR.
(ii) The CAR discovery solution SHOULD be able to verify that such an AR is a CAR. In other words, this AR has APs whose coverage areas overlap with at least one AP of the AR the MN is currently receiving its IP connectivity.

3.13.3 SECURE INTER-OPERABILITY WITH IETF PROTOCOLS

Security on CAR information and capabilities distribution MUST conform and inter operate with existing IETF security policies and protocols on the security of routing information distribution.

3.13.4 SECURE EXPRESSION OF MN's REQUIREMENTS TO THE CAR DISCOVERY SOLUTION

The CAR discovery solution MUST provide a secure means of expression of the MN's requirements to the CAR discovery protocol.Security on communication of MN preferences to ARs MUST conform and inter operate with existing IETF security and AAA policies and protocols for host security, where applicable. This requirement is needed in the case when the CAR discovery solution needs to transfer an MN's preferences to the TAR selection algorithm.

4. ACKNOWLEDGEMENTS

The contributions (in alphabetical order) of Hemant Chaskar (Nokia), Steve Deering (Cisco), James Kempf (DoCoMo Labs), Jari T. Malinen (Nokia), Phil Neumiller (Mesh Networks), Hesham Soliman (Ericsson), and Dirk Trossen (Nokia) were valuable in preparation of this document.

5. REFERENCES

[1] MIPv4 Handoffs Design Team,Low Latency Handoffs in Mobile IPv4, draft-ietf-mobileip-lowlatency-handoffs-v4-00.txt, work in progress, February 2001.

[2] MIPv6 handoff Design Team,Fast handoffs for Mobile IPv6, draft-ietf-mobileip-fast-mipv6-01.txt, work in progress, April 2001.

[3] O. H. Levkowetz et. al.,Problem Description: Reasons For Performing Context Transfers Between Nodes in an IP Access Network, draft-ietf-seamoby-context-transfer-problem-stat-01.doc, work in progress, May 2001.

[4] H. Sayed et. al., General requirements for a context transfer framework, draft-ietf-seamoby-ct-reqs-00.txt, work in progress, May 2001.

[5] D. Trossen, G. Krishnamurthi, H. Chaskar, J. Kempf, Issues in candidate access router discover for seamless IP-level handoffs, draft-ietf-seamoby-car-discovery-04.txt,work-in-progress, October 2002.

6. EDITOR'S ADDRESS

Govind Krishnamurthi
Communication Systems Laboratory
Nokia Research Center

5 Wayside Road
Burlington, MA 01803, USA

Phone: +1 781 993 3627
Fax: +1 781 993 1907
E-mail: govind.krishnamurthi@nokia.com