

Requirements for CAR Discovery Protocols
[draft-ietf-seamoby-card-requirements-00.txt](#)

Status of This Memo

This document is an Internet-Draft and is in full conformance with all provisions of [Section 10 of RFC2026](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or made obsolete by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

Copyright Notice

Copyright (c) The Internet Society (2001). All rights reserved.

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.

INTERNET-DRAFT Requirements for CAR Discovery Protocols May, 2002

TABLE OF CONTENTS

1. INTRODUCTION	2
2. TERMINOLOGY	2
3. REQUIREMENTS FOR CAR DISCOVERY PROTOCOLS	
3.1 IDENTIFYING THE IP ADDRESSES OF GAARs	3
3.2 SUPPORT FOR INTER-TECHNOLOGY HANDOFFS	3
3.3 IDENTIFYING GAARS HAVING SITE-LOCAL AND PRIVATE ADDRESSES	4
3.4 CAPABILITY DISCOVERY	4
3.5 UTILIZATION OF NETWORK RESOURCES	4
3.6 FORMAT OF CAPABILITIES	4
3.7 SCOPE OF CAR DISCOVERY	4
3.8 INTRODUCTION OF DEDICATED NETWORK ELEMENTS FOR CAR DISCOVERY	4
3.9 INVOLVEMENT OF NON-GAARs IN CAR DISCOVERY	5
3.10 DEPENDENCE ON A PARTICULAR MOBILITY MANAGEMENT PROTOCOL	5
3.11 EFFECT OF CHANGES IN NETWORK TOPOLOGY	5
3.12 PROVIDING THE MN'S REQUIREMENTS TO THE CAR DISCOVERY SOLUTION	5
3.13 SECURITY REQUIREMENTS	5
3.13.1 SECURE CAPABILITY TRANSFER	5

3.13.2 VERIFICATION OF ROUTER AUTHENTICITY	5
3.13.3 SECURE INTER-OPERABILITY WITH IETF PROTOCOLS	6
3.13.4 SECURE EXPRESSION OF MN's REQUIREMENTS TO THE CAR DISCOVERY SOLUTION	6

Krishnamurthi, Editor

[Page 1]

INTERNET-DRAFT Requirements for CAR Discovery Protocols May, 2002

4. ACKNOWLEDGEMENTS	6
5. REFERENCES	6
6. EDITOR'S ADDRESS	7

[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.

Geographically Adjacent AR (GAAR)

An AR whose coverage area is such that an MN may move from the coverage area of the AR currently serving the MN into the coverage area of this AR. In other words, GAARs have APs whose coverage areas are geographically adjacent or overlap.

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)

This is an AR that is a candidate for MN's handoff. CAR is necessarily a GAAR of the AR currently serving the MN, and also has the capability set required to serve the MN.

Krishnamurthi, Editor

[Page 2]

INTERNET-DRAFT Requirements for CAR Discovery Protocols May, 2002

Target AR (TAR)

This is the AR with which the procedures for the MN's IP-level handoff are initiated. TAR is usually selected from the set of CARs.

TAR Selection Algorithm

The algorithm that determines a unique TAR for MN's handoff from the set of CARs. The exact nature and definition of this algorithm is outside the scope of this document.

[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 GAAR](#)

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 GAAR. 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 GAARs connected to APs of a different technology.

[3.3](#) IDENTIFYING GAARS 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 GAARs 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 GAAR's capabilities. The CAR discovery solution MUST be able to provide the MN with GAAR information along with their capabilities.

[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 GAARs 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 [\[5\]](#), GAARs 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-GAARs IN CAR DISCOVERY

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

[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.

[3.13](#) SECURITY REQUIREMENTS

[3.13.1](#) SECURE CAPABILITY TRANSFER

The CAR discovery solution MUST ensure that the capability information of GAARs is transferred in a secure fashion.

[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 GAAR is a genuine AR.
- (ii) The CAR discovery solution SHOULD be able to verify that such an AR is a GAAR. 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.

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. Levkowitz 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 discovery for seamless IP-level handoffs, [draft-ietf-seamoby-car-discovery-02.txt](#), work-in-progress, January 2002.

INTERNET-DRAFT Requirements for CAR Discovery Protocols May, 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

