Network Working Group
Internet Draft
Intended status: Standards Track
Expires: October 2008

F. Z. Yousaf
C. Wietfeld
Communication Networks Institute,
Dortmund University of Technology,
Germany.
April 23, 2008

Multi-Hop Discovery of Candidate Access Routers (MHD-CAR)
draft-yousaf-ietf-network-mhdcar-00.txt

Status of this Memo

Copyright Notice

Abstract

The Candidate Access Router Discovery (CARD) protocol specified in [1] is aimed to enable seamless IP layer handover by aiding seamless Layer 3 (L3) mobility management protocols like Fast Mobile IP (FMIP) by providing identity and capabilities information of the candidate access routers (CARs) to the mobile node (MN) prior to the initiation of handover while the MN is still connected to its current AR.

The specifications as laid down in [1], however, specifies a very generic mechanism of the CARD protocol effective only in specific network architecture scenarios and it doesn't take into account the stringent requirements of a fast moving MN and real time communication sessions, especially when it comes to resolving candidate access routers that my be adjacent geographically but not topologically.

This draft addresses the expected shortcomings of the base CARD protocol with respect to fast moving MNs and real time communication sessions by proposing extensions that is expected to improve and/or enhance the performance of the generic CARD protocol as specified in [1].

Table of Contents

1. Requirements notation

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [9].

2. Introduction

Next generation network (NGN) is envisaged to be IP based composed of heterogeneous wireless access network architecture catering to a large number of mobile users with varied quality and service requirements.

To accommodate the expected increase in mobile users' population and mobile applications, mobility management protocols, both at the data link layer and network layer are being developed and enhanced to provide and optimum seamless handover to mobile entities.

In this respect, Mobile IPv6 (MIPv6) [2] is a L3 mobility management protocol specified for IPv6 networks, as IPv6 is expected to be the internetworking technology of choice due to its various inherent advantages over its predecessor IPv4, but the delay and packet losses incurred by MIPv6 makes it unsuitable to provide seamless handover to mobile users, especially in terms of the stringent quality of service requirements and demands of the NGN.

Fast-MIPv6 (FMIPv6) is an extension to the base MIPv6 protocol and specified in [3] that is designed to overcome the inherent functional deficiencies of MIPv6 in terms of providing seamless handover to mobile nodes (MNs).

The operational philosophy behind F-MIPv6 is to perform delay incurring sub-processes, such as movement detection and Care-of-Address (CoA) configuration while the MN is still connected to its current access router (AR) and just before it hands over its connection the new AR (NAR). This is only possible if the MN is provided with the identity (L2 and L3 addresses) and capabilities (QoS and other related parameters) information of the candidate access point (CAP) and its associated candidate AR (CAR) well in advance and the degree of seamlessness provided by FMIPv6 is highly dependent on the timely provisioning of the CAR information.

The protocol specifications of FMIPv6 does not specify the mechanics of this advance retrieval of identity and capabilities information of CAR(s) and/or selection algorithm of target AR (TAR), but instead it relies on external protocols/algorithms to achieve this performance target.

Candidate Access Router Discovery (CARD) is one such protocol [1] that enables a MN to discover and acquire the identity and/or capabilities information of CAR(s) prior to the initiation of handover while it is still connected to its current AR. The problem statement of CAR discovery is documented in [4].

Although specified as a separate protocol, the CARD protocol can be easily integrated into the FMIPv6 protocol framework.

The CARD protocol is based on the exchange of a pair of Request/Reply messages between the MN and AR and between AR and AR, every time a MN detects a L2 ID(s) of new in-range AP(s) during link layer scan.

Although an effective strategy, but owing to the frequent exchange of CARD messages during every handover instance, it is expected that the base CARD protocol may not scale well for fast moving MNs (moving at vehicular velocities) in terms of signaling load and timely provision of CAR(s) information; thereby adversely impacting the degree of seamlessness provided by mobility management protocols like FMIPv6 and any TAR selection algorithm(s).

This draft document specifies a mechanism by virtue of which a MN will be able to discover and acquire the identity and capabilities information of CAR(s) "multiple link-hops" away from the current AR incurring minimum signaling load, especially over the wireless link (MN-AR CARD Request/Reply Messages). This mechanism utilizes the original CARD messages with minor modifications and is expected to enhance the performance of the base CARD protocol and thus improve the degree of seamlessness provided by fast handover protocols like FMIPv6.

Although MHD-CAR does not introduce any new messages but it proposes changes to the way the CAR Table information is managed and exchanged, besides introducing a new data structure called "New Access Network (NAN) Cache, which is managed and maintained inside the MN.

3. Terminology

This document refers to [1] and [3] for terminology. The following terms and abbreviations are additionally used in this document.

New Access Network (NAN) Cache:

> A cache maintained by the MN containing identity and capabilities and distance information of the candidate ARs and candidate APs.

4. CARD Protocol Overview

4.1. CARD Protocol Operation Summary

The CARD protocol specifications [1] provides a generic mechanism that allows MNs to resolve the L2 IDs of one or more in-range APs,

typically discovered during a scan operation by the MN, to the IP addresses, and additionally the capabilities, of the associated CARs.

This reverse address translation is carried out by the MN transmitting a MN-AR CARD Request message towards its current AR, which will resolve the L2 IDs of the discovered AP(s), carried by the received request message, to the corresponding CAR's IP addresses by consulting its local CAR Table.

The current AR, after performing reverse address translation and capabilities discovery, will respond by sending a corresponding MN-AR CARD Reply message back to the MN, informing the MN of the resolved CAR(s) IP address(es) and its capabilities. This discovery and acquisition of the CAR(s) identity and capabilities information may be used by the MN to perform TAR selection and/or aid the MN to execute some L3 related handover functions in advance.

The CARD protocol provides for the piggybacking of the CARD messages on fast handover protocol messages.

The CAR Table is fundamental for performing reverse address translation and capabilities discovery. The CAR Table is a L2-L3 address mapping table maintained by each AR. The CAR Table is also provisioned to maintain the capability information of CARs, which is updated periodically depending on the timeout expiry of a capability parameter(s) lifetime or a change in its state and/or value. The CARs also maintains their own AP-to-AR mappings and capability information in the local CAR Tables, in order to aid newly booted MNs to obtain AR'S certification path. The detailed description of the CAR Tables and its entries are not given in the CARD protocol specifications.

The CARD specification also suggests and recommends that a MN SHOULD also maintain discovered address and capability information of the local CARs in a local cache to avoid requesting the same information repeatedly and to select an appropriate TAR from the list of CARs as quickly as possible when a handover is imminent. However the conceptual design and management principle of such a local cache is not part of the official CARD specifications.

The maintenance of the CAR Table and its efficient dissemination is the key stone to CARD operational capabilities. The CAR Table can be configured statically but that is most inefficient. In this respect the CARD protocol proposes two approaches for the maintenance of the CAR Tables in the ARs which are summarized below.

4.1.1. Centralized approach using a CARD Server

The centralized approach uses a CARD Server entity that assists the current AR in performing reverse address translation. This centralized approach requires the "neighboring ARs" to register their identities with the CARD server to populate the reverse address translation table prior to the initiation of any reverse address translation, preferably during a CAR boot up time. When the current AR is unable to resolve a L2 ID as requested by a MN, it will query the CARD server using a AR-Server Request message. In response the CARD server will return the IP address of the resolved CAR and the current AR will also update its local CAR Table for subsequent requests. The current AR will then directly contact the CAR and perform capabilities discovery with it. The initial idea was presented in [5]

The drawback of this approach however is that additional messages (AR-Server Request and AR-Server Reply) are introduced and the CARD server entity introduces a single point of failure in the network. Also it may not be able to resolve CAR(s) which may belong to some different administrator domain, in which case CARD will fail to resolve the CAR and FMIPv6 protocol will not function.

4.1.2. Decentralized approach Using Mobile Node's Handover

The decentralized approach makes use of a mobile terminal's handover. The main idea behind this approach is to bootstrap and maintain the association between two neighboring ARs, with overlapping coverage area, by using the first handover of a MN occurring between them. Subsequent handovers of other MNs will serve to refresh the association between the neighboring ARs.

During the handover, the MN will send a "Router Identity message" to its current AR containing the IP address of the previous AR. This message will allow the current AR to add or update an entry for the previous AR as its neighbor. As a security measure, a reception of a Router Identity message will trigger the current AR to send an AR-AR message to the previous AR containing the IP address of the MN in order to verify its identity. Upon receiving a positive verification, both the neighboring ARs will update their local CAR tables with each others identity and capabilities information using the normal AR-AR CARD Request/Reply messages. This approach was presented in [6] and [7].

The drawback of this approach however is the introduction of a new message (router identity message) and increase in signaling load over the air link and between ARs and the first MN missing on the

advantages offered by seamless handover protocol. Since Router Identity Message is exchanged over the air link, in case of lossy air links or collision the ARs will not be able to maintain credible information.

4.2. Expected Issues Related to FMIPv6 with CARD

FMIPv6 is designed to provide seamless and fast handover to MNs, but the degree of seamlessness depends on the efficiency of CARD protocol and its ability to resolve the CAR(s) identity and/or capabilities information well in advance and with minimum delay and signaling overhead.

FMIPv6 protocol provides two handover modes [3] depending on whether the Fast Binding Acknowledgement (FBAck) message is received by the MN on the previous/current AR's (PAR) link or next/new AR's (NAR) link. In the former case the handover mode is termed "predictive" and in the latter case the handover mode is termed "reactive".

Of the two handover modes the predictive mode is more relevant in terms of the CARD protocol because in this mode the MN is able to resolve the CAR information while it is still connected to PAR, but for high speed MNs, it is highly likely that during the address resolution and/or capabilities discovery delay incurred by CARD, the MN may move out of the range of the current AR and perform L2 handover with NAR before the NAR identity and/or capabilities gets resolved, and the MN undergoes reactive handover mode, in which case CARD protocol is rendered irrelevant. Reactive handover may account for packet losses for the duration when the MN sends a Fast Binding Update (FBU) towards its current AR from the NAR's link and till a reverse tunnel is not established between PAR and NAR.

In case the PAR is unable to resolve the identity of the NAR, the MN will not undergo FMIPv6 handover but revert to MIPv6 handover incurring a higher handover delay associated with MIPv6.

Since the CARD protocol is triggered every time a MN receives L2 IDs from in-range APs, this may not be feasible especially for fast moving MNs, because the MN is usually able to listen to neighboring APs when it is almost on the edge of the coverage area of its current AP and, depending on the area of overlap region, it is possible that the MN may move out of the coverage area of the current AP before it has resolved the NAR identity.

Fast moving MNs undergo a higher frequency of handover and thus CARD protocol is initiated every time a MN is about to handover to a CAR, thus incurring higher signaling load, especially the MN-AR CARD

Request/Reply messages. Since the MN-AR CARD Request/Reply message pair is exchanged over wireless link, they are more error prone than the AR-AR CARD Request/Reply message pair. This may not be suitable for fast moving MNs and/or real time communication sessions, as there is not enough time for retransmissions before a MN moves out of the coverage area of the current AP as explained above.

The evident shortcomings of the CARD protocol with respect to fast moving MNs and real time applications are expected to be rectified by empowering the MN to perform reverse address translation and/or capabilities discovery of CAR(s) that may be multiple link-hops away with minimum reliance on current AR and with minimum exchange of MN-AR CARD Request/Reply message pair. This is achieved by Multi Hop Discovery of Candidate Access Router (MHD-CAR) protocol as discussed and detailed in the next sections.

5. Multi Hop Discovery of Candidate Access Router (MHD-CAR)

MHD-CAR is a protocol aimed at enabling a MN to resolve the identity and capabilities information of CAR(s) that may be geographically adjacent but topologically it may be multiple hops away from the current AR.

One of the main feature of MHD-CAR is the ability of the AR's to dynamically update their local CAR Table with the identity information of not only the neighboring ARs but also CARs located multiple hops away. The MHD-CAR operation does not require maintaining and/or managing a CARD Server or using a MN's handover to bootstrap and refresh the CAR Table of an AR. Instead each AR will maintain a snap-shot of the network around it in its local CAR Table. This CAR Table is dynamically configured at the initialization of the AR and is refreshed routinely.

Also MHD-CAR requires a MN to maintain a local cache called "New Access Network (NAN) Cache", the information content of which enables a MN to resolve a CAR with minimum reliance on MN-AR CARD Request/Reply messages, thereby decreasing the signaling load, especially over the wireless link and attaining signaling and timing efficiency that may contribute towards improving the probability of a fast moving MN to undergo a Predictive FMIPv6 handover.

This distributed approach of MHD-CAR provides a highly scalable, efficient and fault tolerant mechanism by overcoming the inherent shortcomings of the CARD protocol as explained in the previous sections.

The MHD-CAR does not introduce any new protocol messages and utilizes the CARD Request/Reply messages.

It proposes changes to the way the CAR Table information is managed and exchanged, besides introducing a new data structure called "New Access Network (NAN) Cache, which is maintained inside the MN.

The combination of CAR Table and NAN Cache and their management brings the main advantages of MHD-CAR.

The functional details of the MHD-CAR are discussed in the subsequent sections.

5.1. Access Router Operation

As specified in [1], the AR MUST maintain a CAR Table, which is a L2-L3 address mapping table. The arrangement and composition of the CAR Table in MHD-CAR is different from what is suggested in [1] and the details of the CAR Table are elaborated in section 3.1.1.

MHD-CAR introduces a parameter, besides many others discussed in section 3.1.1, called 'Distance' in the CAR Table which is a measure of the distance of a CAR, in terms of the number of link-hops, from the local AR which is maintaining the CAR Table.

ARs exchange their CAR Table information with their neighboring ARs using AR-AR CARD Request/Reply message pair [1]. Each AR-AR CARD Reply message will carry the CAR Table information of the source AR in the capability container message sub-option.

The exchange of CAR Table information with the neighboring ARs takes place with the iterative exchange of unsolicited AR-AR Reply message, where the number of iterations is equal to the specified maximum distance for which the ARs are supposed to maintain the CAR Table.

At initialization, each AR will populate its CAR Table with its own identity and capabilities information and set the 'Distance' parameter to zero. The 'Distance' of zero indicates local AR information. Each AR will then exchange its local CAR Table entries with its neighboring ARs using unsolicited AR-AR CARD Reply Message.

In the first iteration, the ARs will exchange their local [AP-ID, AR-Information] tuples, and optionally capabilities information, with their neighboring ARs, which will add this new information to their local CAR Tables and increment the 'Distance' by 1. Now each AR will have AR information about their neighboring ARs and this will be

indicated by the 'Distance' value of 1, meaning that the neighboring ARs are at a distance of one link-hop away.

This new update of the local CAR Tables will prompt the ARs to start the second iteration at random times of sending unsolicited AR-AR Reply messages which will contain the updated new CAR Table information in the capability container sub-option. The receiving ARs will compare the new information with the present CAR Table entries and if no match is found, will add the new CAR information to its local CAR Table by incrementing the distance parameter of all received entries by 1. This new entry will thus be stored in the local CAR Table with the 'Distance' value of 2, indicating that the relevant CAR is at distance of two link-hops away.

This new update of the local CAR Tables will prompt the ARs to start the third iteration and this iterative exchange of local CAR Table information with the neighboring ARs will continue until each AR has the information about CAR which is MAXIMUM_DISTANCE_LIMIT away. The value of the MAXIMUM_DISTANCE LIMIT is a constant that depends on the network topology and can be specified by the administrator. How ever the optimum value of the MAXIMUM_DISTANCE LIMIT constant is under investigation.

After the MAXIMUM_DISTANCE_LIMIT iterative exchange of unsolicited AR-AR Reply massages, the CAR Tables will converge. It should be noted that the CAR information (identity and capabilities) are carried in the capabilities container sub-option along with the 'Distance' information, and the AR-AR messages are only exchanged with their neighbors and ARs are not supposed to forward this message, or else the network can get flooded with these messages.

After the convergence of CAR Tables that happens during the ARs initialization/bootup stage, the AR can send out an unsolicited AR-AR Reply message if there is any change in its capabilities or identity information or if a lifetime value of an entry expires, which will again be iteratively distributed amongst ARs MAXIMUM_DISTANCE_LIMIT away. It is expected that the CAR Tables will converge with minimum time without producing excessive traffic on the network links, where the time of convergence is a function of MAXIMUM_DIST_LIMIT.

5.1.1. CAR Table Conceptual Design

As specified in [1] each AR must maintain a CAR Table which is a L2-L3 address mapping table maintaining a [AP-ID, AR-Info] tuple. The AP-ID mainly contains the address of the AP connected to the router, whereas the AR-Info is the router's valid L2 address, IP address and prefix of the interface to which the AP is connected to.

However MHD-CAR proposes additional parameters to the CAR Table.

The parameters defined for the AP-ID field are as follows:

- L2 ID: The L2 ID of the CAP associated with the corresponding CAR. Usually the 6 Byte MAC Address of the CAP.
- L2 Type: Determines the type of access technology (i.e, WiAMX, WLAN, CDMA, UMTS, GPRS, etc,).
- Channel Number: The channel/frequency of the CAP.
- SNR (RSSI): The SNR (or RSSI) of the received beacon.

The parameters defined for the AR-Info field are as follows:

- IP Address: The valid IP address (IPv4 or IPv6) of the interface to which the AP is connected to.
- IP Prefix: The prefix of the IP address of the interface to which the AP is connected to.
- Prefix Length: The prefix length of the IP address of the interface to which the AP is connected to.

MHD-CAR introduces the capability container to the CAR Table and the following parameters are defined for it:

- Bitrate: The bit rate supported by the CAP.
- SSID: The identity of the CAP.
- Distance: The distance of the CAR/CAP from the current AR in terms of link-hops.

5.2. Mobile Node Operation

The CARD specification [1] proposes that a MN SHOULD maintain discovered address and capability information of CARS in a local cache to avoid requesting the same information repeatedly and to select an appropriate target AR from list of CARs as quickly as possible when a handover is imminent, but this proposal will only quicken the CAR selection if the MN has visited that CAR domain previously, whereas it is very much unlikely for a fast moving user to revisit a previously visited CAR domain before the corresponding entry times out. The conceptual design and arrangement of this local cache however is not specified in [1].

In MHD-CAR the MN MUST maintain a local cache, called "New Access Network (NAN)" cache. The NAN cache maintains information of the CARs that will aid the MN in selecting the appropriate CAR for handing over its connection to, when the handover is imminent. The information contents of the NAN cache is derived mostly from the CAR Table that is either "pushed" in the MN by the current AR, or either "pulled" by the MN from its current AR. The NAN cache also derives some of the information contents from the beacon messages received from the in-range wireless APs.

The MN can "Pull" the CARD Table from the current AR by sending a wildcard MN-AR CARD Request Message, in response to which the current AR will append the necessary CAR(s) information in the various sub-options of the MN-AR CARD Reply Message. On the other hand the current AR upon sensing the connection of the MN to itself will send an unsolicited MN-AR CARD Reply Message containing the CAR(s) information appended as various sub-options. Whether the CAR information is pulled by or pushed in the MN, the MN will add and/or refresh the relevant entries of its NAN Cache based on the information provided by the MN-AR CARD Reply Message.

The NAN Cache will contain the identity and capabilities information of not only the neighboring CAR(s) but of CAR(s) MAXIMUM_DISTANCE_LIMIT away from the current AR. This will allow the MN to perform reverse address translation and capability discovery without the exchange of MN-AR CARD Request/Reply message pair whenever handover is imminent. This will not only reduce the signaling load over the wireless link and improve the probability of resolving a CAR but also reduce the delay incurred due to reverse address translation and capability discovery procedure being carried out locally within the MN without having to perform signal exchange with the AR.

Besides relying on MN-AR Card Reply message for keeping it up to date, the NAN Cache will also depend on the L2 information that it receives periodically in the form of beacons from in-range wireless APs. The NAN Cache in essence is a repository that maintains both L2 and L3 information regarding CAR(s). The information content of the NAN Cache will be used by the MN to enhance the performance of both L2 and L3 mobility management mechanisms and thus potentially lays the foundation of a cross-layer mobility management schemes.

5.3. New Access Network Cache Conceptual Design

The information in the NAN Cache is keyed by the L2 ID(s) that the MN receives from the beacon signals of the in-range CAPs. The NAN Cache

entries provide information that can also potentially aid TAR selection algorithms.

The proposed NAN Cache is composed, but not limited to, the following parameters/fields for every CAR:

- Reachability Status: Indicates whether a MN is reachable (attached) to the AP signified by the particular NAN Cache entry.
- Context ID: A context id used to match the information exchange between correct CARD Request/Reply message pair.
- L2 Type: Determines the type of access technology (i.e, WiMAX, WLAN, CDMA, UMTS, GPRS, etc,).
- L2 ID: The L2 ID of the CAP associated with the corresponding CAR. Usually the 6 Byte MAC Address of the CAP.
- SSID: SSID of the CAP
- Bit Rate: The bit rate supported by the CAP.
- Channel Number: The channel number/frequency of the CAP. This entry can be used by selective frequency scanning algorithms to reduce the latency due to scanning delay (For example Probe delay in 802.11 networks).
- SNR: The signal to Noise ratio of the CAP. This entry continues to get updated with every received beacon. Can be potentially used to determine the appropriate time of initiating handover with the next CAP/CAR.
- Receive Power: Receive power of the CAP. This entry continues to get updated with every received beacon. Potentially used to determine the direction of movement of the MN relative to the "reachable" AP and/or CAP. Also aid in the decision to select the appropriate Target AR (TAR) to handover to.
- First Beacon Timestamp: The time a beacon was received from the AP to which this entry belongs.
- Last Beacon Timestamp: Records the time stamp of the latest beacon received for the corresponding CAP/CAR. This entry continues to get updated with every received beacon. The information for maintaining the timestamp of the beacons for the corresponding CAP will allow the MN to determine the dwell time and the period for which it remains in the range of a particular CAP.

- IP Address Type: Indicates whether the CAR identity information is based on IPv4 or IPv6.

- IP Address: The IP address of the interface of the CAR which is connected to the CAP. Its size is 32 bits in case of IPv4 and 128 bits in case of IPv6. Used internally

- IP Address Prefix: The prefix of the CAR's IP Address.

- IP Address Prefix Length: The prefix length of the IP Address. Stored as an integer.

- Capability Container: A data structure that contains the capability information, such as QoS parameters and buffer size of the corresponding CAR.

The information content of NAN Cache also improves the performance of the L2 handover by aiding selective frequency scanning and thus provides both L2 and L3 information for a combined efficient and a true cross layer mobility management solution.

The AR receiving an unsolicited AR-AR CARD Reply message will add or update its local CAR Table with the information contained in the capability container sub-option, and will increment the 'Distance' field for each new received entry by 1. The ARs will continue this inter exchange of their CAR Table with each other through unsolicited AR-AR CARD Reply messages until the CAR Tables converge.

The CAR Tables will converge with several inter-exchanges of the AR_AR Reply messages during boot up time as described previously.

6. Security Considerations

Security issues for this document follow those for CARD protocol.

7. IANA Considerations

See [8] for instructions on IANA allocation

8. Acknowledgments

This document was prepared using 2-Word-v2.0.template.dot.

9. Normative References

[1] M. Liebsch, A. Singh, H. Chaskar, D. Funato, "Candidate Access Router Discovery (CARD)", RFC 4066, July 2005.

[2] Johnson, D., "Mobility Support in IPv6", RFC 3775, June 2004.

[3] Koodli, R., Ed., "Fast Handover for Mobile IPv6", RFC 4068, July 2005.

[4] Trossen, D., Krishanmurthi, G. Chaskar, H., Kempf, J., "Issues in candidate access router discovery for seamless IP-level handoffs", Work in Progress.

[5] D. Funato et al., Geographically Adjacent Access Router Discovery Protocol, Internet draft, draft-funato-seamoby-gaard-01.txt, June 2002.

[6] Shim, E. and R. Gitlin, "Fast Handoff Using Neighbor Information", Internet Draft, draft-shim-mobileip-neighbor-00.txt, November 2000.

[7] Trossen, D., et al., "A Dynamic Protocol for Candidate Access-Router Discovery", Internet draft, draft-trossen-seamoby-dycard-01.txt, March 2003.

[8] J. Kempf, ``Instructions for Seamoby and Experimental Mobility Protocol IANA Allocations," RFC 4065, Internet Engineering Task Force, June 2004.

[9] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

Author's Addresses

Faqir Zarrar Yousaf,
Communication Networks Institute
University of Dortmund
Otto-Hahn-Str. 6,
D-44227 Dortmund, Germany

Email: faqir.yousaf@tu-dortmund.de

Christian Wietfeld,
Communication Networks Institute
University of Dortmund
Otto-Hahn-Str. 6,
D-44227 Dortmund, Germany

Email: christian.wietfeld@tu-dortmund.de

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.