AUTOCONF Working Group
Internet-Draft
Intended status: Informational
Expires: April 29, 2010

C. Bernardos
UC3M
R. in 't Velt
TNO
October 26, 2009

Addressing Model for Router Interfaces in Ad Hoc Networks
draft-bernardos-autoconf-addressing-model-01

Status of this Memo

Copyright Notice

Abstract

This document describes a practical IP addressing model for interfaces that take part in router-to-router communications in ad

hoc networks.

Requirements Language

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 RFC 2119 [RFC2119].

Table of Contents

1. Introduction

In order to communicate among themselves, ad hoc routers [RFC2501] need to configure their network interface(s) with addresses that are valid within an ad hoc network. Ad hoc routers may also need to configure globally routable addresses, in order to communicate with devices on the Internet. From the IP layer perspective, an ad hoc network presents itself as a L3 multi-hop network formed over a collection of links.

This document describes a practical addressing model for ad hoc networks. It is required that a such model does not cause problems for ad hoc-unaware parts of the system, such as standard applications running on an ad hoc router or regular Internet nodes attached to the ad hoc routers.

2. Terminology

Readers are expected to be familiar with all the terms defined in the RFC 2501 [RFC2501]. In addition the document makes use of the following definitions:

Wireless Link

According to [I-D.iab-ip-model-evolution], a "link" in the IP service model refers to the topological area within which a packet with an IPv4 TTL or IPv6 Hop Limit of 1 can be delivered. That is, where no IP-layer forwarding (which entails a TTL/Hop Limit decrement) occurs between two nodes. A "wireless link" can be defined similarly, with the topological area in this case given by the radio-range coverage of the wireless technology used. Due to the nature of the wireless medium, links are intermittent, and potentially short-lived. Node movement exacerbates these characteristics.

MANET interface

Any interface over which a MANET protocol is run.

MANET domain

A MANET domain is delimited by a set of MANET routers that run a common MANET routing protocol and corresponds to its routing domain.

Attached MANET (domain)

A MANET domain attached to an infrastructure based network (e.g., the Internet). The MANET interfaces of routers of an attached MANET should be configured with unique global IP addresses, if these addresses are somehow exposed beyond the MANET domain. By infrastructure network, we refer to any existing network which presents a certain hierarchical organisation (e.g., different subnets) and that is delegated a certain set of IP addresses/ prefixes.

Non-overlapping prefix

Two IP prefixes p::/l_p and q::/l_q are non-overlapping if and only if there is no IP address p::a/l_p configured from p::/l_p that also belongs to q::/l_q, and the other way around. For example, 2001:DB8:1:1::/64 and 2001:DB8:1:2::/64 are non-overlapping prefixes, while 2001:DB8:1::/48 and 2001:DB8:1:2::/64 are not.

3. Addressing model

This section describes a practical IPv4/IPv6 addressing model for ad hoc networks. We first define the scope of the addressing model, then propose how to practically configure IP on MANET interfaces. Finally, we provide some considerations on address uniqueness.

3.1. Scope

This document describes an addressing model for MANET interfaces. Regular (non-MANET) interfaces are not in the scope of the present document, as they are expected to be configured using standard mechanisms (such as SLAAC [RFC4862] or DHCP [RFC2131], [RFC3315]). Note, that MANET routers may need to acquire IP address prefixes to facilitate the configuration of IP addresses on nodes reachable via non-MANET interfaces. How to do this is a topic that is also outside the scope of this document.

This document does not place restrictions on the use of IP addresses configured on MANET interfaces. We assume that these IP addresses are used by MANET routing protocols. We also assume that, once MANET routing protocols have started to populate the Forwarding Information Bases (FIB) of routers with routing entries, these IP addresses will play a role in the forwarding of user data packets. In particular, it is assumed that these addresses will be found as next-hop addresses in the routing tables of MANET routers. The forwarding of user data in many cases includes the resolution of the link-layer address of the interface to which the next-hop IP address is bound. Furthermore, it cannot be ruled out that the IP addresses configured

on MANET interfaces will be used as source or destination addresses by end-user applications in cases where such applications reside on MANET routers. An architecture in which applications are separated by one hop from MANET interfaces is conceptually elegant, but may not always be practical.

This document considers MANET domains for the purposes of IP configuration. Therefore, when we use the term "MANET" throughout this document, we are referring to a MANET domain. For example, MANET local uniqueness refer to uniqueness within the MANET domain.

Globally unique IP addresses MUST be provided for routers of attached MANETs for those cases where these addresses are visible outside the MANET domain, while only uniqueness within the MANET domain is required for non-attached MANETs.

This document does not rule out that IP addresses might be configured by non-autoconf mechanisms (e.g., manually) on MANET interfaces.

3.2. IPv4/IPv6 practical addressing model

This section describes the basic principles for IP addressing for MANET interfaces, in as much an IP version agnostic manner as possible.

MANET interfaces of attached MANETs SHOULD be configured with global IPv6 addresses if these addresses are somehow exposed outside the MANET domain. For non-attached MANETs, ULAs or global addresses SHOULD be used.

Since the topology of a mobile ad hoc network is expected to be frequently changing, MANET interfaces MUST be configured with unique/non-overlapping prefixes. This principle does not assume any prefix length. The use of /32 (in the IPv4 case) or /128 (in the IPv6 case) prefix lengths can be an effective way to ensure that prefixes are non-overlapping. However, it would be needlessly restrictive to mandate the use of only these prefix lengths. Due to its larger address space, it is much easier to generate addresses for IPv6 that are unique than is the case for IPv4. This is equally true for prefixes with non-maximum lengths.

MANET interfaces MUST also be configured with IPv6 Link-local addresses (as required by RFC 4861 [RFC4861] and RFC 4291 [RFC4291]). Two main concerns may arise when considering the use of IPv6 Link-local addresses:

- Address uniqueness: the event of having two duplicate addresses in the same link has proved to be very low (EUI64 derived interface

identifiers very rarely collide, since MAC addresses are expected to be globally unique), and even some mechanisms have been proposed to reduce the collision probability [paper.DAD]. Therefore, in most scenarios it is safe to assume that the probability of having two or more duplicated link-local addresses in a MANET is negiglible. For those scenarios, in which this cannot be safely assumed, we refer to the DAD considerations of Section 3.3.

- Reachability: connectivity among neighbours in wireless links may be intermittent and/or short-lived. Therefore, the use of link-local addresses may lead to reachability issues, since two nodes that were in direct coverage range at one moment, might not be anymore shortly after. These problems might also arise in wired networks (nodes going up/down), but it is not the common case.

Designers of MANET routing protocols (and other protocols) should be aware of these concerns and assess their impact, in order to make an informed decision whether to make use of link-local addresses or not.

Fluctuating reachability as discussed above is also of concern to the data forwarding process in ad hoc networks. This is especially true, if existing mechanisms for neighbour discovery and address resolution are to be applied. In order to mitigate these problems, several solutions may be used, such as (but not limited to): decrease some of the ND default timer values (specified in RFC 4861 [RFC4861]), such as REACHABLE_TIME, RETRANS_TIMER, DELAY_FIRST_PROBE_TIME, MIN_RANDOM_FACTOR, MAX_RANDOM_FACTOR; implement a stronger interaction between the MANET routing protocols and the ND process, so the MANET routing protocol helps to keep updated the ND tables. Finally, if none of these solutions (or alternative ones) may be implemented, processes running on the MANET routers that need to be isolated from this problem can decide not to use link-local addresses for their local communications. Since IPv4 lacks any standardised unreachability detection mechanism, these considerations about reachability only concern IPv6.

Configuration and use of IPv4 link-locals on MANET interfaces are not forbidden. However, while in IPv6, an interface may be simultaneously configured with a link-local address and with unicast (global or local) addresses, this is not recommended in IPv4 [RFC3927].

When forwarding user data packets from one MANET router to the next, along the path from source to destination, standard mechanisms for layer-2 address resolution of next-hop IP addresses, such as ND or ARP, may be used. In this context, it should be noted that the presence of IPv6 link-local addresses on MANET interfaces may lead to

their use, e.g. as source address in a neigbor solicitation. As mentioned before, the exchange of MANET routing protocols packets is a potential alternative source of link-layer address information.

3.3. DAD considerations

This document assumes that DAD is disabled by default for the IP addresses configured on MANET interfaces (this is allowed in RFC 4862 [RFC4862]. For the case of link-local addresses, we assume the collision probability is negiglible, and that it therefore is safe to avoid the overhead of an active DAD process (which would need to be modified to be run in a MANET domain wide fashion). For the case of the non-overlapping prefixes, we do not specify how their uniqueness is ensured (this is out-of-scope of this document and falls in the solution space).

However, this document does not forbid the use of any DAD mechanism, if it is required in some certain scenarios. From the point of view of MANETs, it seems appropriate to consider as well the use of passive DAD approaches (such as [paper.PACMAN], [paper.PACMAN_assessment]).

4. IANA Considerations

This document makes no request of IANA.

5. Security Considerations

This document does currently not describe any security considerations.

6. Acknowledgements

Some of the ideas included in this draft have been proposed in the AUTOCONF ML by several people. Thanks for all the AUTOCONF WG participants for the fruitful discussions over these years.

The authors would like to thank Thomas Clausen and Teco Boot for their comments and discussion on this document.

The research of Carlos J. Bernardos leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n. 214994 (CARMEN project) and also from the Ministry of Science and Innovation of Spain, under the QUARTET project (TIN2009-13992-C02-01).

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC2131] Droms, R., "Dynamic Host Configuration Protocol", RFC 2131, March 1997.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3927] Cheshire, S., Aboba, B., and E. Guttman, "Dynamic Configuration of IPv4 Link-Local Addresses", RFC 3927, May 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

7.2. Informative References

[I-D.iab-ip-model-evolution] Thaler, D., "Evolution of the IP Model", draft-iab-ip-model-evolution-01 (work in progress), November 2008.

[RFC2501] Corson, M. and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, January 1999.

[paper.DAD] Bagnulo, M., Soto, I., Garcia-Martinez, A., and A. Azcorra, "Avoiding DAD for Improving Real-Time Communication in MIPv6 Environments", Joint International Workshop on Interactive Distributed Multimedia Systems/ Protocols for Multimedia Systems IDMS-PROMS 2002, Coimbra (Portugal). Lecture Notes in Computer Science 2515, pps 73-79, Ed. Springer-Verlag, 2002. , November 2002.

[paper.PACMAN]
Weniger, K., "PACMAN: passive autoconfiguration for mobile ad hoc networks", IEEE Journal on Selected Areas in Communications 23 (3) , 2005.

[paper.PACMAN_assessment]
Bernardos, C., Calderon, M., Soto, I., Solana, A., and K. Weniger, "Building an IP-based Community Wireless Mesh Network: Assessment of PACMAN as an IP Address Autoconfiguration Protocol", Computer Networks, accepted for publication , 2009.

Authors' Addresses

Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30
Leganes, Madrid 28911
Spain

Phone: +34 91624 6236
Email: cjbc@it.uc3m.es
URI: http://www.it.uc3m.es/cjbc/

Ronald in 't Velt
TNO Information and Communication Technology
Brassersplein 2
Delft 2600 GB
The Netherlands

Phone: +31 15 2857306
Email: Ronald.intVelt@tno.nl