Autoconf
Internet-Draft
Intended status: Informational
Expires: August 29, 2009

T. Clausen
U. Herberg
LIX, Ecole Polytechnique
February 25, 2009

MANET Router Configuration Recommendations
draft-clausen-manet-autoconf-recommendations-00

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

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 obsoleted 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/1id-abstracts.txt.

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

This Internet-Draft will expire on August 29, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract

This document describes a pragmatic set of configuration recommendations for MANETs, as well as provides a rationale for why

these recommendations are sound. While there may be other equally valid ways of configuring a MANET, the recommendations in this document have the merit of being supported by an existence proof (there're running networks in existence, configured according to these recommendations), and they require neither modifications to the IP stack nor to upper-layer protocols or applications.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

Table of Contents

1. Introduction 3
   1.1. Document Outline 4
2. MANET Configuration Recommendations 4
   2.1. MANET "Node" Morphology -- Hosts and Routers 5
   2.2. MANET Interface Configuration 6
   2.3. Prefixes delegated to MANET Router 7
3. Example MANET Configurations 7
   3.1. MANET Router and Single Host 7
   3.2. MANET Router and Attached Network w. Prefix Delegation . . 9
   3.3. MANET Router and Attached Network w/o Prefix Delegation . 10
   3.4. MANET Router with two MANET Interfaces and Attached Network 11
4. Rationale 12
   4.1. Unique MANET Interface Addresses 13
   4.2. /32 and /128 Prefix Lengths 14
   4.3. IP Hop Isolation 18
5. Summary and Characteristics 20
6. IANA Considerations 21
7. Security Considerations 21
8. Acknowledgments 21
9. References 22
   9.1. Normative References 22
   9.2. Informative References 22
Authors' Addresses 22

1. Introduction

A MANET (Mobile Ad hoc NETwork) is, in academic circles, commonly described as a variation over the following:

"a collection of independent nodes, communicating over a wireless, capacity-restricted medium, whereby they form a multi-hop connected network with no assumptions of an a-priori network infrastructure and with a highly dynamic topology."

While such a description may be extrapolated to interesting challenges for research and protocol design, such as fast-convergence routing algorithms and bandwidth-economic protocols, it does little to describe the exact morphology and IP configuration of the "independent nodes" from which the MANET is constructed. Consequently, it offers little guidance in how a "real-world" IP-based MANET can be configured and deployed.

MANET routing protocol specification as developed by the IETF, such as [RFC3626], [RFC3561], [RFC4728] and [RFC3684], stipulate internal processing of such "independent nodes" as well as specify the exact protocol message exchange between these, in order to allow construction of routing tables. As such, these specifications allow for operation of a MANET, and do provide indications as to under which assumptions such operation is assumed -- but on the other hand do not have as vocation to provide explicit configuration and deployment guidelines for MANETs. MANET routing protocols explicitly assume that all MANET nodes in a MANET are already configured, i.e. that the network interfaces have appropriate IP addresses etc.

The purpose of this present document is to remedy that by describing recommendations and considerations for configuring and deploying a MANET. These considerations are characterized by adhering strictly to IP -- i.e. to require no modifications to neither the protocol stack nor to applications accessing the network -- and to be applicable for, to the best of the authors knowledge, any MANET using any choice of routing protocol from among those developed for MANETs within the IETF.

Caveat lector: Other configurations and deployment approaches for MANETs are likely possible, and should not be disregarded or excluded. This document, however, describes a set of configuration and deployment recommendations, which practical experience and real-world deployments have shown to be feasible. Also note that this document describes only the end result -- but not any process (automatic or otherwise). Hence, when the term "configuration" is employed, it is as a noun for "the end result".

1.1. Document Outline

Section 2 presents, without rationale, explanation or apologies, recommendations for the constitution and configuration of a MANET router and of a MANET. This should allow the reader to immediately understand how to -- safely -- configure and deploy an IP based MANET using any of the currently developed IETF MANET routing protocols. This, while maintaining compatibility with all "Internet applications" and with other protocols, and without requiring modifications to the IP stack.

Section 3 shows a selection of MANET router configurations, each strictly following the recommendations given in Section 2. These examples are not exhaustive, but rather illustrative for the kind of deployments supported by the recommendations in Section 2.

Section 4 explains the background and rationale for the configuration recommendations presented in Section 2. For each configuration recommendation, a selection of justifications are presented and detailed. This should allow the reader to understand why the recommendations given in Section 2 represent a reasonable and operational way of configuring a MANET.

Section 5 concludes this document by summarizing the configuration recommendations and the characteristics of a MANET configured according to the recommendations given in this document.

2. MANET Configuration Recommendations

This section presents a small set of MANET configuration recommendations. As indicated in Section 1, these recommendations constitute an approach for which there is an existence proof that a MANET so configured is both correctly functioning and one in which "Internet applications" and other protocols operate unmodified without requiring modifications to the IP stack.

Section 2.1 expands the notion of MANETs being constructed from "independent nodes" into the familiar terminology on the Internet and of IP networking of "Hosts" and "Routers".

Section 2.2 describes address configuration of MANET router interfaces, and Section 2.3 how prefixes delegated to a MANET router are used.

Caveat lector: This section explains uniquely the HOW of configuration of a MANET router and a MANET. The WHY -- the rationale and justification -- is given in Section 4.

2.1. MANET "Node" Morphology -- Hosts and Routers

Each "independent node" in a MANET can functionally be described according to Figure 1, with the "MANET node" being composed of a "MANET router" (R) with one or more "MANET interfaces" -- i.e. the interface which is to be used for establishing connectivity between MANET routers -- as well as zero or more interfaces towards other networks or hosts on classic IP links.

```
                                \|/
                MANET interface  |
                     +-----------|---------------------+
                     |        +--+------+              |
                     |        |    R    |  MANET router|
                     |        +---------+              |
                     |         |      |                |
                     |      +---+     | Classical IP   |
                     |      | H |     | links with     |
                     |      +---+     | hosts          |
                     |         _______|______          |
                     |        |       |      |         |
                     |      +---+   +---+  +---+       |
                     |      | H |...| H |  | H |       |
                     |      +---+   +---+  +---+       |
                     |                                 |
                     +---------------------------------+
                                 MANET node
```

Figure 1: MANET "node" morphology

Functionally, this entails that:

- o MANET routing protocols are run over MANET interfaces only;
- o MANET routers enable connectivity between the MANET and hosts or other non-MANET networks;
- o MANET characteristics are "isolated behind an IP hop" from hosts or other networks;
- o Applications on hosts and other networks can remain "MANET unaware".

A MANET, therefore, looks as depicted in Figure 2: the inner cloud represents where MANET routers have MANET interfaces and where only MANET aware protocols operate (e.g. MANET routing protocols) -- and the outer cloud represents the non-MANET-aware part of the network, with hosts and other (non-MANET) networks.

```
                        ,.----..      _.--'''--._
              ___    ,'        ``. ,'           `.   _......_
          _,''   ``,'          +---+   +---+      ,-'       `-.
         /                     | H |   | H |                   \
        |                      +---+   +---+                    \
        |                        |_______|                       |
        |                         ____|              Edge        |
        ,                      ,-'    +-.   ___                _.'
      ,'   +---+       ,,---../       |  `''   ``.              ``._
    ,'     | H |--+  ,'            +--+--+        `.                \
    /      +---+  | /  +-----+     |  R  |          \                |
   |              +----|  R  |     +-----+   Core   |                |
   `.      +---+  | '  +-----+    /       \         '                |
    |      | H |--+ /     \      /         \        `.              /
     `.    +---+   |       \  +-----+      +-----+    \           ,'
       `-.         \        \_|  R  |------|  R  |    |        -''.
         /          \         +--+--+      +-----+    '            `.
       ,'            `.          |                  _,'               \
      .'               `-.       | ,`.         ,'''                  |
      |                   `-.___.+'   `..__,,,'                      |
      |                          |                                   /
       \                   ,-----+--.                               /
        \                  |        |                            _,'
         `.              +---+    +---+                     ..,-'
           `-..____,,<   | H |    | H |  /(                /
                      \  +---+    +---+ ,' \              ,'
                       `.              /    `.          ,'
                         `._        ,-'       `-..___,,'
                            ``----''
```

Figure 2: A MANET with routers (R) and hosts (H). The "core" consists of routers that are responsible for network formation and maintenance. The "edge" includes hosts and non-MANET aware networks.

This is akin to, say, an OSPF network, which can be depicted similarly to Figure 2: Within the inner cloud, OSPF routers with NBMA interfaces would be operating using protocol mechanisms suitably aware of NBMA characteristics, whereas the outer cloud would contain non-NBMA-aware parts of the network, such as hosts.

2.2. MANET Interface Configuration

The following summarizes the configuration constraints for MANET interfaces of a MANET router:

- o Each MANET interface on a MANET router MUST be configured with an IP address which is unique, at least within the MANET.

- o Each MANET interface MUST be configured with a prefix length of /32 (for IPv4) or /128 (for IPv6).

2.3. Prefixes delegated to MANET Router

The following summarizes the configuration constraints for a prefix, delegated to a MANET router:

- o If a prefix is delegated to a MANET router, this prefix MUST NOT be configured on any MANET interface.

- o If a prefix is delegated to a MANET router, other (non-MANET) interfaces MAY be configured with this prefix.

3. Example MANET Configurations

This section provides a set of illustrative examples of common MANET configurations, respecting the considerations given in Section 2.2. Notice that this section does not attempt to exhaustively enumerate all possible MANET deployments or configurations.

In the examples below, IP addresses and prefixes are extracted from within the private address space 192.168/16. This is for illustrative purposes only. This document does not take any position as to which address space is to be used for when configuring MANETs or other networks.

3.1. MANET Router and Single Host

Figure 3 illustrates a MANET node consisting of a MANET router with a single MANET interface and a single host. This is the typical case, for example, when one has a laptop, PDA or smartphone participating in the MANET: the "router" and the "host" are in that case logical components within the same device, and with a single physical interface.

The MANET node is assigned a single IPv4 address, in this case 192.168.1.1. This IP address is to identify both the MANET interface of the MANET router as well as the host. Logically, this is accomplished by configuring the interface of the MANET router as an "unnumbered interface", by assigning 192.168.1.1/32 to the MANET interface of the router. Traffic to the logical component that is the router will typically be addressed to a well-known multicast address, thus the router can distinguish between traffic to itself and traffic to the logical host.

```
                                  \|/
                                   | 192.168.1.1/32
                           +-------|--------------+
                           |    +--+--+           |
                           |    |  R  |           |
                           |    +-----+           |
                           |      /               |
                           |     / 192.168.1.1/32 |
                           |  +---+               |
                           |  | H |               |
                           |  +---+               |
                           +----------------------+
```

Figure 3: MANET router (R) and a single internal host (H)

It is important to retain that the MANET interface is configured with a prefix length of /32, as this is an IPv4 network -- had it been an IPv6 network, the required prefix length for the MANET interfaces would have been /128.

For administrative reasons, e.g. for the ability to aggregate routes for injection into other routing domains, IP addresses assigned to MANET interfaces (or prefixes delegated to MANET routers) within the same MANET may be extracted from within a larger interval, say, 192.168.0.0/16. Even so, each MANET interface configured with an IP address MUST be configured with a prefix length of /32 (IPv4) or /128 (IPv6) and no MANET interface may be configured with this larger address interval as prefix. Notice that in this situation, the address interval 192.168.0.0/16 represents the ability to aggregate a set of addresses into a single entry, and is specifically *NOT* related to "subnet" or "subnet prefix".

A complete MANET so configured might look as depicted in Figure 4.

```
                              _____       ,,-''''`-..
                          ,,-'     `-.._-'           `._
       192.168.0.0/16  ,'                               \
                      /                        \|/      \___
                     /           \|/            |           `-.
                    |             |         +---+----+         `.
                    |        +----+---+     |192.168.|           |
                     |       |192.168.|     | 1.2/32 |           |
                    _'       | 1.1/32 |     +--------+           /
                   /         +--------+                         <
                  /                                   \|/      \
                  |                     \|/              |        \
                  \                      |          +----+---+     \
                   \                +----+---+      |192.168.|      |
                    `.              |192.168.|      | 1.4/32 |      |
                      `-..__.       | 1.3/32 |      +--------+     /
                            \       +--------+                    /
                             `.                                  ,'
                               `.         _,.                ,,-'
                                 `--....-'   `..         ,,'
                                                `'-----''
```

Figure 4: A correctly configured MANET. IP addresses within the routers are those assigned to the MANET interface. Notice that while all such IP addresses are extracted from the address interval 192.168.0.0/16, all MANET interfaces are configured with prefix lengths of /32.

3.2. MANET Router and Attached Network w. Prefix Delegation

Figure 5 illustrates a MANET router with a single MANET interface and an interface towards a classic IP link such as an Ethernet. The MANET router is delegated the IPv4 prefix 192.168.1.0/24. That prefix is assigned to the non-MANET link, on which interfaces are assigned addresses such as 192.168.1.1/24, 192.168.1.2/24, 192.168.1.3/24 etc. Note that the interfaces on that classic IP link are configured with a prefix length of /24, indicating that the interfaces with addresses from within that IP prefix are all reachable within a single IP hop.

The MANET interface is configured as an "unnumbered interface" by "borrowing" the address (192.168.1.1) from its interface towards the classic IP link - but is configured with the prefix length /32. The MANET interface is, specifically, not configured with a prefix length of /24, even though that prefix is delegated to the MANET router, as the MANET interface is not able to reach all other interfaces with addresses from within 192.168.1.0./24 in a single IP hop.

```
                 192.168.1.1/32  \|/
                     +------------|------------+
                     |            |            |
                     |          +-+-----+      |
                     |          |   R   | 192.168.1.0/24
                     |          +-------+      |
                     |192.168.1.1/24 |         |
                     |               |         |
                     +---------------+---------+
                                     |
                          ,----------+-----------.
                          |          |           |
                       +---+      +---+       +---+
         192.168.1.2/24 | H |      | H |       | H | 192.168.1.4/24
                       +---+      +---+       +---+
                             192.168.1.3/24
```

Figure 5: MANET router (R) with an attached network and a delegated subnet prefix. Notice that the prefix 192.168.1.0/24 is assigned to the non-MANET link, where interfaces are configured with that prefix, e.g. 192.168.1.3/24. The MANET interface "borrows" the IP address from that link, however is configured with a prefix length of /32.

Traffic to the MANET interface with the IP address 192.168.1.1 can be distinguished from traffic to the non-MANET interface with the same address since traffic destined to the MANET interface of the router typically will be addressed to a well-known multicast address.

3.3. MANET Router and Attached Network w/o Prefix Delegation

Figure 6 shows a situation similar to that of Section 3.2 except that the MANET router, for whatever reason, is not delegated any prefix.

As no prefix has been delegated to the MANET router, the MANET router can not simply "borrow" an IP address from within a delegated prefix for its MANET interface and know this IP address to be unique -- but has to rely on some other mechanism for acquiring an IP address. Whichever mechanism is used for acquiring this IP address, is shall ensure that this IP address is unique, at least within the MANET.

Assuming that the MANET router has acquired the IP address 130.225.194.42 for use on its MANET interface, and that whatever mechanism gave this IP address to the MANET router ensured that this address is unique, at least within the MANET, then the MANET router can be configured as in figure Figure 6.

```
                    130.225.194.42/32  \|/
                           +------------|------------+
                           |            |            |
                           |          +-+-----+      |
                           |          |   R   |      |
                           |          +-------+      |
                           |               |         |
                           |               |         |
                           +---------------+---------+
                                           |
                                ,----------+-----------.
                                |          |           |
                             +---+      +---+       +---+
                             | H |      | H |       | H |
                             +---+      +---+       +---+
```

Figure 6: MANET router (R) with an attached network. The router has, through whichever mechanism, acquired the IP address 130.225.194.42 -- with which it configures its MANET interface and with a prefix length of /32. At this time, no prefix is delegated to the MANET router.

The MANET router may attempt to acquire a prefix, through whatever mechanism availble on the network, for use when configuring attached hosts and networks -- or may assign IP addresses from within a private address space to such hosts and networks, and deploy NAT.

3.4. MANET Router with two MANET Interfaces and Attached Network

Similar to Figure 5, Figure 7 illustrates the configuration of a MANET router with two MANET interfaces. In this case, the attached network and one of the MANET interfaces is configured exactly as in Figure 5, whereas the second MANET interface is configured using an otherwise unused IP address -- in this case 192.168.1.42 -- from within the 192.168.1.0/24 prefix. This interface is also configured with a prefix length of /32.

```
                192.168.1.1/32  \|/ \|/  192.168.1.42/32
                    +------------|---|--------+
                    |            |   |        |
                    |          +-+---+-+      |
                    |          |   R   | 192.168.1.0/24
                    |          +-------+      |
                    |192.168.1.1/24 |         |
                    |               |         |
                    +---------------+---------+
                                    |
                         ,----------+-----------.
                         |          |           |
                       +---+      +---+       +---+
       192.168.1.2/24 | H |      | H |       | H | 192.168.1.4/24
                       +---+      +---+       +---+
                             192.168.1.3/24
```

Figure 7: MANET router (R) with an attached network and a delegated subnet prefix and two MANET interfaces. Notice that the prefix 192.168.1.0/24 is assigned to the non-MANET link, where interfaces are configured with that prefix, e.g. 192.168.1.3/24. The MANET interface "borrows" the IP address from that link, however is configured with a prefix length of /32. The second MANET interface is configured using an unused IP address from within the same subnet prefix, in this case 192.168.1.42 -- also configured with a prefix length of /32

Using IP addresses from within the prefix delegated to the MANET router for configuring MANET interfaces on that router ensures that these IP addresses are unique, at least within the MANET -- assuming, of course, that the prefix delegation mechanism does not delegate the same prefix to multiple MANET routers within the same network.

Notice that the same logic applies in this scenario as in the one in Figure 5: the second MANET interface could assume any IP address from within 192.168.1.0/24, even one already used by a host such as 192.168.1.2, as long as it is not used on another MANET interface and as long as the second MANET interface is also configured with a prefix length of /32. Traffic to the MANET interface with the IP address 192.168.1.2 can be distinguished from traffic to the non-MANET interface with the same address since traffic destined to the MANET interface of the router typically will be addressed to a well-known multicast address.

4. Rationale

Section 2 describes three recommendations when configuring MANET

routers and MANET interfaces on MANET routers:

- o Each MANET interface on a MANET router MUST be configured with an IP address which is unique, at least within the MANET;

- o MANET interfaces MUST be configured with prefix lengths of /32 (IPv4) or /128 (IPv6);

- o MANET routers MUST isolate MANET characteristics from non-MANET interfaces.

This section provides a rationale for the configuration recommendations in Section 2 by presenting the reasoning behind each of these -- as well as a selection of consequences from configuring a MANET router without following these recommendations.

In the descriptions in the following sections, IP addresses and prefixes are extracted from within the private address space 192.168/16. This is for illustrative purposes only. This document does not take any position as to which address space is to be used for when configuring MANETs or other networks.

4.1. Unique MANET Interface Addresses

MANET interfaces are typically not attached to point-to-point links, but are rather of a "semi-broadcast nature" such as indicated in Figure 8. Hence, a packet transmitted on a MANET interface may be received by any number of MANET interfaces, including the transmitting MANET interface itself.

```
                    Communication
                        Range
                <~~~~~~~~~+~~~~~~~~~> <~~~~~~~~~+~~~~~~~>
                          |<~~~~~~~~~+~~~~~~~~~>|
                       +--|--+   +--|--+   +--|--+
                       |  A  |   |  B  |   |  C  |
                       +-----+   +-----+   +-----+
```

Figure 8: Example of "semi-broadcast" MANET interface characteristics. The arrows indicate the transmission range for each MANET interface, i.e. the range within which a transmitted packet can be successfully received and decoded.

In order for MANET routers to be able to forward data packet not destined to themselves or to directly attached non-MANET hosts or networks, they need to be able to uniquely identify the "next hop" for a packet. Symmetrically, in order for a MANET router to discriminate between incoming data packets for it to forward (either

within the MANET or to an attached host or network) or to discard, it needs to be able to identify if indeed it is the "next hop" for a received data packet. In order to accomplish this, MANET interfaces which are in direct L2 communication with each other need to be configured with unique IP addresses.

Some MANET routing protocols employ flooding mechanisms (also commonly denoted "optimized flooding") in order to reduce the overhead involved in topology dissemination throughout the network. Examples include [RFC3626] and [RFC5449]. Such flooding mechanisms are based on each node selecting a subset of its neighbors as "relays", with only these relays taking part in flooding operations. Such relay selection algorithm in general require the ability to uniquely identify each MANET interface up to two hops away from the source; such is the case for [RFC3626] and [RFC5449].

Other flooding algorithms, studied for MANETs, perform relay selection requiring the ability to uniquely identify each MANET interface further away -- such is the case with various non-connected dominating set flooding approaches, currently a subject of research.

By configuring MANET interfaces such that each has a MANET-wide unique address, it is ensured that both the flooding mechanisms from the current crop of MANET routing protocols, as well as potential future developments, are supported.

4.2. /32 and /128 Prefix Lengths

In early MANET deployments, a common occurrence was to configure a MANET as "a subnet" and configure it as indicated in Figure 9: the MANET would have a subnet prefix, say 192.168.1.0/24 and MANET interfaces would be configured with this subnet prefix, e.g. 192.168.1.3/24.

```
                   Communication
                       Range
           <~~~~~~~~~~~~~+~~~~~~~~~~~~~> <~~~~~~~~~~~~~+~~~~~~~~~~~~~>
                        |<~~~~~~~~~~~~~+~~~~~~~~~~~~~>|
                    +--------+    +--------+    +--------+
                    |192.168.|    |192.168.|    |192.168.|
                    | 1.1/24 |    | 1.2/24 |    | 1.3/24 |
                    +--------+    +--------+    +--------+

       Data packet:     -------------->
        dest     192.168.1.3
        next-hop 192.168.1.2

         ICMP Redirect  <--------------
```

Figure 9: Misconfigured MANET: MANET interfaces configured with a shared /24 prefix, causing the central router to produce an ICMP redirect when forwarding packets from 192.126.1.1 to 192.168.1.3.

If, for example, a data packet was transmitted by the MANET router 192.168.1.1 to be received by 192.168.1.3, then this would -- with reference to Figure 9 -- have to be forwarded by the MANET router 192.168.1.2. With the MANET interfaces in this MANET being configured with the subnet prefix 192.168.1 and the prefix length /24, it was observed that this produced ICMP redirects by 192.168.1.2.

An early, and often suggested, solution was to "treat the symptoms rather than cure the disease" by disabling ICMP redirects on MANET routers -- i.e. to require modifications to the IP stack operation in order that it can be supporting MANETs.

The ICMP redirect is intended to be used to inform a source to send packets using an alternative, more direct, route -- e.g. if a source, s wishes to send a data packet to a destination node d via the path s-R1-R2-d, and if R1 knows that a direct path s-R2-d is available, then the ICMP redirect from R1 will inform s of this route.

Two interfaces, configured with addresses from within the same subnet prefix, and with the same prefix length are defined to be reachable from each other within a single IP hop. More precisely, it is assumed that all interfaces with IP addresses within that subnet prefix and configured with the same prefix length are directly reachable from each other without forwarding by an intermediate router. Hence, a way for R1 to know that a direct path may exist between h and R2 is if h, R1 and R2 are configured with IP addresses from within the same subnet prefix and within the same subnet prefix.

Returning to the MANET scenario in Figure 9, with all MANET interfaces being configured with the same subnet prefix and the same prefix length, it follows from the discussion above that all these MANET interfaces are expected to be directly reachable from each other within a single IP hop. When, in this configuration, the router 192.168.1.2 is requested to forward a data packet from 192.168.1.1 to 192.168.1.3, it is expected that it generates an ICMP redirect to 192.168.1.1 suggesting that a direct path exists from 192.168.1.1 to 192.168.1.3 -- as this is what the configuration suggests.

Rather than "treating the symptoms" and disabling ICMP redirects, requiring /32 and /128 prefix lengths on MANET interfaces "cures the disease". An interface so configured will not make any assumptions about other interfaces being within a single IP hop, and so will not generate ICMP redirects when forwarding traffic.

An argument could be made, suggesting that for each set of MANET interfaces which are all directly reachable in one IP hop from each other, a shared "subnet prefix" can be assigned. Considering the network from Figure 9, this could allow two "subnets" to be formed, as indicated in Figure 10, with the MANET interface of the center router being configured with two IP addresses (or, being configured with two virtual interfaces, each with one IP address), one in each of the two subnets.

```
                                   .
           Communication           .
               Range               .
       ~~~~~~~~~~~~+~~~~~~~~~~~~~~~~~><~~~~~~~~~~~~~~~~~~~~+~~~~~~~~~
                   <~~~~~~~~~~~~~~~~~+~~~~~~~~~~~~~~~~~~~~>
                                   .

             192.168.1.1/24        .              192.168.2.2/24
                 \ | /           \ | /               \ | /
                  \|/      192.168. \|/ 192.168.        \|/
                   |        1.2/24   |   2.1/24          |
                +--|-+            +----+            +--|-+
                | N1 |            | N2 |            | N3 |
                +----+            +-.--+            +----+
                                   .
              ----------------------.
              Subnet prefix        .--------------------------
                     192.168.1.0/24 .     Subnet prefix
                                   .            192.168.2.0/24
```

Figure 10: MANET interfaces configured with a shared /24 subnet prefixes among neighbors which can all communicate directly in one IP hop. Notice that some MANET interfaces will be required to have multiple IP addresses, and as the network topology changes, also change their MANET interface configuration.

While this could be a valid configuration, considering that the "M" in MANET is for "mobile", the network topology can be expected to change dynamically and frequently. A network so configured would, therefore, require constant "subnet formation" and "interface reconfiguration", in order to maintain the configuration valid. It would require (complex) mechanisms for tracking the topology dynamics and would entail potentially frequent changes to MANET interface address configurations. Such frequent changes of interface configurations would likely also adversely affect e.g. relay selection mechanisms such as those used for flooding in [RFC3626] and [RFC5449]: from the point of view of a router R, even if the topology within a 2 hop radius from R did not physically change (and so, no relay set recalculations would be needed), the logical configuration of interface addresses on a node 2 hops away from R might change (e.g. due to physical topology changes to the neighborhood of that node, i.e. 3 hops away from R) in order to preserve the ability of having "shared prefixes" among neighboring MANET interfaces. This would then potentially require relay set recalculations by R and additional signaling to this effect by a routing protocol on R -- even though topological changes were 3 hops away from R and such recalculations and signaling would not be necessary in case MANET interface addresses were kept stable.

Finally, as the only application(s) to be exposed to MANET interfaces are MANET routing protocols and other protocols explicitly MANET aware and designed for management of a MANET infrastructure, it is highly questionable if there would be any benefits from introducing the complexities necessary for maintaining such dynamically changing "subnets" among MANET interfaces.

Configuring MANET interfaces with a /32 or /128 prefix length is, therefore, a safe approach which entails no additional complicated mechanisms or signaling, and which requires no changes to the IP stack.

4.3. IP Hop Isolation

Upper-layer applications and protocols are designed with a set of (often not explicitly expressed) assumptions as to the nature and characteristics of the underlying network communications fabric. This includes, but is not limited to, assumptions on (i) the relationship between a "subnet" and the ability for interfaces configured within the same subnet to all be able to communicate with each other directly, i.e. in one IP hop (as evoked in Section 4.1 and Section 4.2), (ii) that communication between interfaces on the same link is symmetric (if interface A can receive packets from interface B, then interface B can receive packets from interface A), (iii) that link-local multicast (i.e. with TTL or hop-limit equal to 1) is supported and is well defined (e.g. that the recipients of a link local multicast from interface A is identical to those of interface B, assuming that interfaces A and B are on the same link). Essentially, upper-layer applications and protocols assume an underlying link with characteristics similar to those of an Ethernet.

Over MANET interfaces, these assumptions may not hold true. Consider for example the network in Figure 11. If interface A makes a link local multicast transmission, then this is received by the interface B -- whereas if interface B makes a link local multicast transmission, then this is received by the interfaces A and C.

```
                    Communication
                        Range
               <~~~~~~~~~+~~~~~~~~~> <~~~~~~~~~+~~~~~~~>
                        |<~~~~~~~~~+~~~~~~~~~>|
                     +--|--+   +--|--+   +--|--+
                     |  A  |   |  B  |   |  C  |
                     +-----+   +-----+   +-----+
```

Figure 11: Link local multicast over MANET interfaces: without forwarding, a transmission from the manet interface A reaches a different set of interfaces than those for a transmission from

interface B (or interface C).

There are, essentially, four potential ways of addressing this problem: requiring all upper-layer applications and protocols to become "MANET aware", inventing mechanisms for presenting a MANET as-if it was an Ethernet, pushing the problem to layer 2, or encapsulating any MANET specific behavior in a way such that it is only exposed to explicitly MANET aware applications and protocols.

Requiring all upper-layer applications and protocols to be reworked such that they be MANET aware is impossible, due to the sheer volume of such, is undesirable as a tenant of the Internet is to provide an abstraction for applications from the interconnect characteristics, and would likely, not be without technical problems of its own -- for example, Section 4.2 exposes the complexity with respect to the single problem of correctly ensuring the relationship between "subnet" and which MANET interfaces are able to directly communicate.

Pushing the problem to layer 2, and requiring a layer 2 to present an "Ethernet-like" medium would for a given layer 2 solve the problem -- but do away with the ability to deploy heterogeneous MANETs, and would be akin to e.g. requiring OSPF to do away with all but one interface type and require all layer 2's over which OSPF is expected to run to adhere to this single remaining interface type.

The last way of addressing this problem is to encapsulate MANET specific behaviors in a way such that it only is exposed to explicitly MANET aware applications and protocols. This approach has several merits, not the least of which is that this is exactly the way in which existing routing protocols are deployed: interfaces between routers, and their characteristics, are exposed only to applications and protocols which are explicitly aware of these interfaces and their characteristics, with all other applications and protocols being isolated from these by being connected via an "Ethernet-like" link to the router -- i.e. by virtue of being isolated behind an IP hop (the router).

For example, applications on hosts are exposed to an "Ethernet-like" link with other hosts and potentially routers -- and are blissfully unaware whether these routers are connected using point-to-point links, NBMA links, broadcast links etc.

For these reasons, configuring a MANET such that the MANET router is isolating the MANET interfaces and their characteristics from hosts and other (non-MANET) networks by an IP hop, and requiring that on MANET routers, only explicitly MANET aware applications are exposed to MANET interfaces, is a safe and simple approach that entails no additional complex mechanisms and signaling. This also requires no

changes to neither the IP stack nor the upper-layer applications and protocols operating on these hosts and (non-MANET) networks.

5. Summary and Characteristics

This document proposes recommendations as to how MANETs can be configured and deployed, specifically, it provides the following three sets of recommendations:

MANET Interface Address Configuration:

- o Each MANET interface on a MANET router MUST be configured with an IP address which is unique, at least within the MANET.

- o Each MANET interface MUST be configured with a prefix length of /32 (for IPv4) or /128 (for IPv6).

Delegated Prefix Configuration:

- o If a prefix is delegated to a MANET router, this prefix MUST NOT be configured on any MANET interfaces.

- o If a prefix is delegated to a MANET router, other (non-MANET) interfaces MAY be configured with this prefix.

MANET Interface Characteristics Encapsulation:

- o MANET interface characteristics are exposed only to explicitly MANET-aware protocols and applications, such as MANET routing protocols;

- o MANET interfaces are not exposed to applications and upper-layer protocols, i.e.;

- o MANET routers provide connectivity to hosts and other (non-MANET) networks via links with "Ethernet-like" link characteristics, and;

- o MANET routers provide connectivity from hosts and other (non-MANET) networks via IP routing, i.e. MANET interface characteristics are "hidden behind an IP hop" from applications and upper-layer protocols.

A MANET configured according to these recommendations has the following key characteristics:

MANET Characteristics:

- It requires no modifications to the IP stack on hosts and non-MANET aware networks;
- It requires no modifications to the IP stack on MANET routers;
- It requires no modifications to upper-layer applications and protocols on hosts and (non-MANET) routers;
- It supports all MANET routing protocols, as currently developed within the IETF.

6. IANA Considerations

This document has no actions for IANA.

7. Security Considerations

This document does currently not describe any security considerations.

8. Acknowledgments

The considerations presented in this document are the authors condensation of years of experience within and outside the IETF, from studying, building, testing and deploying MANETs.

The authors would like to express his profound thanks to (in no specific order) Dave Thaler (Microsoft), Thomas Narten (IBM), Jari Arkko (Ericsson), Mark Townsley (Cisco), Chris Dearlove (BAE Systems), Justin Dean (NRL), Joe Macker (NRL), Ian Chakeres (CenGen), Charles E. Perkins (WiChorus), Emmanuel Baccelli (INRIA), Henning Rogge (FGAN) and Ryuji Wakikawa (Toyota) for having given their valuable time to participating in the (at time vivid) discussions with the authors, and forming the foundation for writing this present document.

Emmanuel Baccelli (INRIA) provided valuable proof-reading of this document in its final stages.

9. References

9.1. Normative References

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

9.2. Informative References

[RFC3561] Perkins, C., Belding-Royer, E., and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing", RFC 3561, July 2003.

[RFC3626] Clausen, T. and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", RFC 3626, October 2003.

[RFC3684] Ogier, R., Templin, F., and M. Lewis, "Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)", RFC 3684, February 2004.

[RFC4728] Johnson, D., Hu, Y., and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4", RFC 4728, February 2007.

[RFC5449] Clausen, T., Baccelli, E., Nguyen, D., and P. Jacquet, "OSPF Multipoint Relay (MPR) Extension for Ad Hoc Networks", RFC 5449, February 2009.

Authors' Addresses

Thomas Heide Clausen
LIX, Ecole Polytechnique

Phone: +33 6 6058 9349
Email: T.Clausen@computer.org
URI: http://www.ThomasClausen.org/

Ulrich Herberg
LIX, Ecole Polytechnique

Phone: +33 1 6933 4126
Email: ulrich@herberg.name
URI: http://www.herberg.name/