Mobile Ad hoc Network Architecture

draft-ietf-autoconf-manetarch-07

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with Section 6 of 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 May 11, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document discusses Mobile Ad hoc NETworks (MANETs). It presents the initial motivation for MANET and describes unaccustomed characteristics and challenges. It also defines a MANET, other MANET entities, and MANET architectural concepts.
Table of Contents

1. Introduction ................................................. 3
2. Terminology .................................................. 3
   2.1. Borrowed Terminology ............................... 3
   2.2. MANET Terminology ................................. 4
3. MANET Motivation Discussion ............................... 6
   3.1. Packet Radio Networks .............................. 6
   3.2. Packet Radio Networks and the Internet .......... 6
   3.3. Packet Radio Networks and MANETs .................. 7
4. MANET Interface Characteristics ............................ 8
   4.1. Qualities - Wireless, Mobile, Ad hoc ............. 8
   4.2. Challenges ........................................... 8
      4.2.1. Semi-Broadcast Interface ..................... 8
      4.2.2. Fuzzy Relationships Between Nearby MANET Routers &
              MANET Routers’ Extended Neighborhoods ........ 9
      4.2.3. MANET Membership ................................ 10
5. Addressing & the MANET Prefix Model ........................ 11
   5.1. General Address Architecture ...................... 12
   5.2. MANET Interface Configuration ..................... 13
   5.3. Routers and Hosts in a MANET ....................... 13
6. MANETs’ Place in the Network Stack ........................ 14
7. Sharing of Information Across Layers ........................ 15
8. Deployment Taxonomy ........................................ 15
   8.1. Service Availability ................................ 15
   8.2. Number of MANET Routers in a MANET ............... 16
9. Security Considerations ..................................... 16
10. IANA Considerations ....................................... 17
11. Acknowledgments .......................................... 17
12. Informative References .................................. 18
Authors’ Addresses ........................................... 19
Intellectual Property and Copyright Statements ............... 20
1. Introduction

A Mobile Ad hoc NETwork (MANET) consists of a loosely connected domain of routers. A MANET is characterized by inclusion of one or more MANET interfaces; interfaces that are distinguished by their potentially significant time-vary asymmetric reachability amongst neighboring routers. These routers organize and maintain a routing structure among themselves. These routers may communicate over dynamic wireless channels with asymmetric reachability, may be mobile, and may join and leave the network at any time. These MANETs’ characteristics create challenges in several areas.

This document is focused on IP networking, though many of MANETs’ concepts and issues span the protocol stack.

This document is meant to complement [RFC2501] in describing and defining MANET.

2. Terminology

Owing to the fact that a MANET, as described in this document, is an instance of an IP network, much of the terminology employed in this document is borrowed from existing documents. Some of the documents that contain relevant terminology are [RFC1812], [RFC2328], [RFC2453], [RFC2460], [RFC4861], [RFC4291], [RFC3753], and [RFC4903]. In some cases the terminology is slightly abbreviated or rephrased; although, every effort made to retain the meanings. Borrowed terminology is provided in Section 2.1 with the intent of providing a complete discussion of MANETs using coherent terminology. MANET specific terminology is provided in Section 2.2.

2.1. Borrowed Terminology

This document employs the following definitions:

Node (N)
any device (router or host) that implements IP.

Router (R)
a node that forwards IP packets not explicitly addressed to itself.

Host (H)
any node that is not a router, i.e. a host does not forward packets addressed to others.
Link
a communication facility or medium over which nodes can
communicate at the link layer, i.e., the layer immediately below
IP. Examples are Ethernets (simple or bridged), PPP links, X.25,
Frame Relay, or ATM networks as well as internet (or higher) layer
"tunnels", such as tunnels over IPv4 or IPv6 itself.

Asymmetric Reachability
Asymmetric reachability describes two properties of certain
interface types' underlying communication facilities. First, non-
transitive communication means packets from X can reach Y, and
packets from Y can reach Z, but packets from X may not reach Z.
Second, non-bidirectional communication means that packets from X
can reach Y but packets from Y may not reach X. Many radio/
wireless interfaces exhibit these properties.

Neighbor
In the context of routing, two routers are neighbors if one can
send/receive routing protocol IP packets to the other without
passing through any intermediaries at the same layer.

Interface
A node’s point of attachment to a communication link.

Semi-Broadcast Interface (SBI)
A broadcast capable interface that may exhibit asymmetric
reachability. Multiple access wireless radio interfaces are often
SBI. Note that since a SBI "may" exhibit asymmetric reachability,
it also may not.

Routing Domain (Domain)
A routing domain is an interconnected network with a coherent
routing policy and a consistent metric framework.

Border Router (BR)
A border router participates in multiple routing domains, and
often multiple routing protocols. A BR defines the border between
its multiple routing domains. A BR is responsible for presenting
a consistent picture of the nodes reachable through itself to each
routing domain. A BR determines the routing information to
propagate between different routing domains.

2.2. MANET Terminology

The following terminology is specific to MANETs:
MANET Interface
A MANET interface is distinguished by its potentially significant
time-varying asymmetric reachability (e.g., SBI) amongst potential
neighboring routers. A more detailed discussion of MANET
interface characteristics is presented in Section 4.2. The
addressing constraints for a MANET interface are discussed in
Section 5.2.

MANET Router (MNR)
A MANET router is distinguished by having one or more MANET
interfaces. A MANET router may also have zero or more non-MANET
interfaces. A MANET router is responsible for hiding MANETs’
challenging characteristics from nodes that are not MANET-aware.
A MANET router with a single MANET interface is illustrated in
Figure 1.

MANET Neighborhood
A set of neighboring routers that can communicate via MANET
interfaces without passing through any other routers
(intermediaries at the same layer).

MANET
A routing domain containing MANET routers. A example MANET is
illustrated in Figure 3.

Figure 1: MANET Router with One MANET Interface

Dependent upon the deployment and management strategy, coalescing and
fragmentation of MANETs may be a supported feature. In other words,
if a communication path between two previously separated MANET
routers or MANETs becomes available, the two MANETs may merge to form
a single larger MANET. Similarly, if a communication path between
two MANET routers disappears and no alternative path between the
routers exists, then the MANET may be partitioned into two separate
MANETs.

When discussing MANETs’ connectivity to other networks, such as the
Internet, a MANET is bounded by border routers (BR). That is, a
MANET’s BR form a border between a MANET and other routing domains.
3. MANET Motivation Discussion

The Internet Protocol (IP) core design tenets -- connectionless networking and packet-based forwarding -- are ideally suited for use in highly dynamic contexts, such as MANETs. Yet, some additional functionality is required to meet the unique challenges and opportunities present in MANETs.

3.1. Packet Radio Networks

The initial motivation for MANETs was called Packet Radio (PR) networking [FL01]. In PR, each router is equipped with a single wireless interface. Each router may be mobile, and the routers may be or may become spatially distributed such that all routers cannot communicate directly. That is, two routers might require one or more intermediate routers to forward (route) packets on their behalf. In the example shown in Figure 2: for PR1 to send packets to PR3, the intermediary PR2 must relay the packets. This implies that PR2 must receive the packet from PR1 on its interface and determine that it must retransmit the packet over the same interface as the one where the packet was received, in order for the packet to reach PR3. From the point of view of PR2, both PR1 and PR3 are neighboring routers, whereas PR1 and PR3 are not themselves neighboring routers of one another.

| Communication Range | <---------+--------> | <---------+--------> |
|---------------------|---------------------|
| Single              | <---------+--------> |                     |
| MANET               | ++-+-              | ++-+-               |
| Interface           | [PR1] | [PR2] | [PR3] |                      |
|                     | +++-   | +++-  | +++-  |                     |

Figure 2: Basic Packet Radio Network

3.2. Packet Radio Networks and the Internet

Packet Radio networks inspired several architecture related challenges, including how to interconnect Packet Radio networks and other networks, especially fixed networks like the ARPANET. Another related challenge was how to deal with the large disparity between different node and interface characteristics present in different networks.

These aspects of Packet Radio networks helped stimulate the early development of the Internet Protocol; an architecture based on
connectionless networking and packet-based forwarding that enables interconnection of heterogeneous devices over heterogeneous communication technologies.

3.3. Packet Radio Networks and MANETs

The router configuration in Figure 1 is the simplest MANET router configuration: a single interface exhibiting MANET interface characteristics. Many other challenges exist, in MANETs and in Packet Radio Networks both: wireless interfaces imply shared communication resources which result in interdependence between nearby nodes, and these nodes often communicate directly or indirectly. Wireless channel statistical dynamics and node mobility may result in frequent packet channel losses and network topology changes.

Figure 3 shows a general schematic of a MANET: each MANET Router (MNR) has one or more MANET interfaces, over which MANET interface aware protocols operate to ensure MANET communication; and zero or more non-MANET participating interfaces, either towards hosts or other networks. Over these non-MANET aware interfaces protocols need not be aware of MANETs’ characteristics.

```
+----+
| MNR |
++----+
++  ----+ /  /  \
|    |MNR---  .-.  ---MNR .. |
++  ----+  \
+-+( MANET )-. /  +++

Other (Communication)
Nodes ‘-(______)-’
and \|/  \|/
Networks ++-+-  ++-+-
 | MNR |
++-+-+  +-+-+  +--++
 :  MNR :  
+++-++  ++-++  +++
++  ;  +++
+++
```

Figure 3: Mobile Ad Hoc NETwork Example
4. MANET Interface Characteristics

Inheriting from Packet Radio as described above, primary particularities of MANETs are the characteristics and qualities of MANET interfaces, and the challenges these entail for protocol design and development.

4.1. Qualities - Wireless, Mobile, Ad hoc

In MANETs several qualities impact protocol design. The most fundamental qualities are wireless interface characteristics, mobility, and ad hoc interaction.

Wireless interfaces often exhibit more challenging characteristics when compared to wired interfaces. Many protocols (e.g., IPv6 neighbor discovery [RFC4861]) were not designed to operate in wireless networks with asymmetric reachability. Wireless interfaces may also exhibit very dynamic time varying performance (e.g., packet loss, data rate), and the factors have a significant impact on local communication.

Mobility can also exacerbate communication issues, making it more challenging to attain, establish, and maintain network relationships between nodes.

Ad hoc networking further compounds problems by allowing nodes to join and leave the network, or even form new networks, at will.

4.2. Challenges

MANET characteristics result in many challenges. These challenges reveal themselves in many forms, and MANET specific protocols must often be developed.

4.2.1. Semi-Broadcast Interface

Given a wireless SBI that exhibits time-varying asymmetric reachability and spatially distributed MANET routers, each MANET router may have a different unique partial view of the MANET. That is, each node may see a different set of neighboring MANET routers.
The possibly unique set of neighboring MANET routers perceived by each MANET router often requires MANET routers to send packets out the same wireless interface as the one over which they were received. Topologically, this act of forwarding out the same interface may cause a packet to reach a different set of MANET routers by traversing the wireless communication medium in a new location. An example is provided in Figure 4, where each MANET router is capable of reaching a different set of MANET routers.

The act of forwarding packets out of the same interface as the one over which they were received often results in duplicate IP packets being received by MANET routers with more than one neighboring MANET router, while also reaching a new subset of MANET routers. Thus, duplicate packet detection is often an inherent part of MANET protocol designs.

4.2.2. Fuzzy Relationships Between Nearby MANET Routers & MANET Routers’ Extended Neighborhoods

Defining the process of determining neighboring MANET routers’ existence, continued existence, and loss of existence is a fundamental challenge in MANETs. Relationships with neighboring MANET routers are hard to define due to the MANET interface characteristics.

Historically, two nodes are either neighbors or not neighbors and several simple mechanisms have been used to determine neighbor relationships: single packet reception, acceptable loss rates, and simple handshakes. [RFC4861], for example, employs an initial exchange of messages to determine neighborship or absence thereof. In networks with MANET interface the types of neighbor relationships expand, as do the mechanisms to detect and maintain the state of such
relationships.

Wireless network interfaces may exhibit unidirectional communication. Dynamic wireless networks may also experience significant time varying packet delivery between the same pair of wireless network interfaces, so simple loss rates may not be sufficient to define a neighbor relationship. Similarly, as nodes (and, hence, interfaces) move relatively to each other, past loss rates may not reflect future communication capabilities.

In MANETs' with SBI, MANET routers within the same small geographic region are often densely connected with other nearby MANET routers. These routers form a set of extended neighbor relationships. This set is referred to as a MANET neighborhood. A MANET neighborhood is typically composed of several MANET routers, with each MANET router being densely connected to other MANET routers.

These more dynamic neighbor relationships do not sit well with certain Internet Protocols designed assuming a fixed Ethernet like model to communication links (bidirectional, transitive, and stable). Given the fuzzy neighbor relationships between MANET routers, the addressing model often associated with a Ethernet link is not logical. For example, in an Ethernet network nodes are often told that a particular range of addresses are "on-link". In MANETs’ a MANET router often cannot make assumptions that a particular set of MANET routers is always (directly) reachable. Instead, MANET routers must detect and determine neighboring MANET routers, and handle changes to this set over time.

4.2.3. MANET Membership

Given MANETs’ characteristics (mobile, wireless, ad hoc), determining a MANETs’ membership is difficult, if not impossible in certain scenarios.
At one moment a MANET might consist of a certain set of nodes, and the next the MANET could partition into several MANETs. Later it might re-merge or merge with a new set of nodes and form a larger MANET.

Certain routers in a MANET might connect to other routing domains. These routers are called Border Routers (BRs), and they often run multiple routing protocol instances. BRs are responsible for choosing the routing information to announce between the various attached routing domains. BRs should also present a consistent picture of the nodes reachable through them.

As MANET membership changes, so does the connectivity of BRs within the MANET. Therefore, a BR may be challenged to present a consistent set of reachable nodes. It may even choose not to announce any routing information about the MANET to other routing domains.

5. Addressing & the MANET Prefix Model

This section presents an architectural model for MANETs which preserves the integrity of the conventional IP addressing architecture while allowing for the particularities of MANET interfaces.
5.1. General Address Architecture

This architectural model considers MANET routers as simply routers with nodes possibly attached. These attached nodes may be attached "behind the router"; that is, the router may be responsible for announcing the location of a particular address or set of addresses (i.e. a subnet prefix).

This configuration implies that, from the point of view of these nodes and the applications running on them, they are not exposed to the specific characteristics of MANET interfaces.

A MANET router can be delegated zero or more prefixes. For example, if a MANET router is delegated a prefix p::, then subnet prefixes derived from this prefix (e.g. p::/64, p::/64, ...) may be assigned to the MANET routers' non-MANET interfaces(s), and nodes on these interfaces may be assigned addresses from within this prefix, and configured with this prefix according to the address autoconfiguration mechanisms governing these interfaces ([RFC4861] and [RFC4862]). This concept is illustrated in Figure 6.

MANET interfaces are specifically *NOT* configured with this prefix. The configuration of these MANET interfaces is detailed in Section 5.2.
5.2. MANET Interface Configuration

MANET interface specific behaviors are exclusively exposed to the MANET routers. These behaviors may include asymmetric reachability, semi-broadcast interfaces, fuzzy MANET router neighbor relationships, changing MANET membership, rapid topology dynamics, etc.

The following characteristics deserve particular mention, since they distinguish the configuration and behavior of MANET interface(s):

Unique Prefixes

MANET interfaces that are known to exhibit the above mentioned properties must be configured with unique prefixes. The reason for this requirement is so that no two MANET interfaces are configured to appear within the same IP prefix. One way to achieve this is /128 (IPv6) or /32 (IPv4) prefixes. It is worth noting that prefix lengths shorter than /128 (IPv6) or /32 (IPv4) are possible on the MANET interfaces, as long as the prefixes are unique to a single MANET interface. Note that the above statements are not an exception, but simply a clarification that MANET are no different from other networks in this respect.

Link-local Multicast/Broadcast Scope

On a MANET interface, a packet sent to a link-local multicast or all-ones broadcast address reaches the MANET interfaces of neighboring MANET routers, regardless of their configured addresses. Link-local multicast/broadcast packets are never forwarded and since a MANET may span several hops, nodes cannot assume that a packet sent to a link-local multicast/broadcast address will reach all routers within a MANET.

5.3. Routers and Hosts in a MANET

The MANET addressing model presented in this section makes a clear separation between the role of MANET router and host in a MANET, recognizing that:

- MANET interface characteristics are only exposed to MANET-aware routers running appropriate protocols;
- nodes and networks/subnets on non-MANET interface(s) are not subjected considering MANET characteristics;
- applications on hosts and protocols run unmodified.

MANET protocols are protocols developed to work on MANET interfaces
Internet-Draft             MANET Architecture              November 2007

and to be MANET-aware. The MANET WG is chartered to develop routing
protocols for MANET interfaces. The Autoconf WG is chartered to
develop autoconfiguration protocols for MANET interfaces and MANET
routers.

Note that this addressing framework is similar to how routing in the
existing Internet is structured. Routers run their routing protocol
over router interconnects with various characteristics to which only
the routing protocols are privy. On the other hand, hosts connect to
routers over interfaces with well-defined characteristics.

6. MANETs’ Place in the Network Stack

While the MANET WG is focused on network (L3) routing, that does not
imply that MANETs and their protocols are limited to L3. Several
previous and existing efforts are applying MANET protocols at various
layers. Many of the challenges discussed above (with the notable
exception being IP addressing) exist independent of at which layer
MANET protocols are deployed. Of course, the protocols themselves
may need to be retooled slightly to accommodate the information
available to the deployed layer.

One example of sub-IP MANET routing is MANET MAC layer (L2) routing.
This type of routing is often called bridging, and may work in
homogeneous wireless networks for delivering frames over multiple
hops.

L2 routing/bridging hides the multiple L2 hops from L3. This
behavior can be advantageous as this network can transparently mimic
an Ethernet, to some extent. The ability to mimic Ethernet allows
the L2 MANET to utilize existing L3 network protocols. On the other
hand, this transparency may lead to performance problems. For
example, if the L3 protocols make heavy use of broadcast messaging or
if devices assume that high-speed bandwidth resources are available.

L2 MANETs do not enable heterogeneity. That is, a L2 MANET is not
capable of bridging across heterogeneous interfaces. For example, L2
bridging cannot directly bridge two L2 technologies with different
addressing schemes. It can also be difficult if the frame sizes of
two L2 technologies vary, as this could require breaking a single
frame into multiple frames of a different format.

L3 MANETs enable heterogeneous networking, as IP was built with this
feature in mind. Forming a MANET at L3 implies that the L3 protocols
must handle the challenges presented in this document.

MANET like protocols can also be used at other layers, both above and
Sharing of Information Across Layers

In wireless networks, and especially in MANETs, propagation of additional information across layers should be considered. For example, link layer feedback that a packet/frame was not able to be sent or that it was not received could be used by the network layer to indicate that a neighboring MANET router is no longer reachable. This information and other extended interfacing could reduce, or eliminate, some upper layer messaging. Further, it could significantly reduce the latency in decision making. Note that though certain lower layer information is valuable, it likely needs to be extrapolated or filtered before accurate assumptions about the network state can be made. For example, failure to deliver a single frame/packet by itself may not be a good indicator that a node is or is not reachable.

In networks with several different layers of MANET mechanisms, the sharing of information across different layers can be even more vital to creating and maintaining the network. For example, if a P2P network is run on top of a L3 MANET, the two networks can share information to use a similar optimized topology, or two network can share neighboring MANET router state changes to reduce the messaging or the latency in making decisions.

Deployment Taxonomy

The present and future proliferation of inexpensive wireless interfaces continues to stimulate technical interest and developments in the area of MANET for a wide variety of deployment scenarios. In this section, we present several characteristics for describing expected MANET deployments.

Service Availability

Nodes often expect certain services/servers to be available. When describing a deployment scenario, it is important to specify the expected services available and the distance between the participating nodes. In MANET, nodes might assume a service is available locally (within one IP hop) or within a particular scope (one or more IP hops - MANET, site, global). Nodes might assume in certain deployments that no special servers/services are available. Finally, nodes might assume that servers are sometimes available, but their availability is not guaranteed or ensured.
Different frameworks for autoconfiguration, network management, and routing within an Autonomous System (AS) can be developed based upon the expected constraints and operating conditions.

8.2. Number of MANET Routers in a MANET

The number of MANET routers in a MANET routing domain is an important consideration. This number is not the complete number of nodes in a MANET (since MANET routers may support an arbitrary number of connected nodes) but a measure of the number of MANET routers participating as a cohesive flat routing domain.

While the number of MANET routers does not define scalability of a MANET protocol, it is often useful to discuss the number of MANET router to get a feel for maturity of typical deployment solutions. For simplicity we define the following network sizes to aid in discussion:

Small
2-30 MANET routers

Moderate
30-100 MANET routers

Large
100-1000 MANET routers

Very large
Larger than 1000 MANET routers

As of 2007, small and moderate size peer MANET routing scenarios have matured and have undergone reasonable test and deployment experience. MANETs of those sizes can perform reasonably well in many cases without hierarchy. For scaling up to large and very large MANET networks, routing hierarchies, a standard technique for wired Internet routing, is a possibility. While scaling design extensions exist, large and very large MANET flat routing domains are still a topic of ongoing active research and are not discussed further here.

9. Security Considerations

Each MANET router may not know its neighborhood a priori (Section 2.2), but it should determine its neighborhood dynamically and track changes as the network evolves. Similarly for MANET network membership (Section 4.2.3), MANET routers may leave or join a MANET, and the MANET may partition or merge with others. In addition to these issues, many MANET routers are expected to communicate over
wireless interfaces; and the "open" nature of wireless communication means that nearby nodes will often be capable of sending and receiving MANET protocol packets.

Without any security measures MANET routers operating under these characteristics will often expose protocol information to and accept information from nearby nodes. Protecting MANET routers from disruptive nearby nodes can be performed by using confidentiality, data integrity, and peer entity authentication.

Different deployments of MANETs may have very different security requirements. For example, if a MANET is deployed for a military purpose, exposing the network topology to any outside party may not be acceptable -- whereas for a civilian deployment exposure of topology information may be of little or no importance. Furthermore, different deployments may require different mechanisms to address security issues (e.g., pre-sharing of keys or certificates), and the MANET routers themselves may have various additional constraints (e.g., computational power for generating or verifying cryptographic attributes). Therefore, due to the large diversity of MANET routers and their deployments, MANET protocols should allow for appropriate, and possibly multiple or various, security mechanisms.

10. IANA Considerations

This is an informational document. IANA requirements for MANET related protocols will be developed within the protocol specifications for MANET protocols.

11. Acknowledgments

Discussions and developments concepts and architectural issues have evolved over many years of discussion of related work within the MANET WG. There are obviously many people that have contributed to past discussions and related draft documents within the WG that have influenced the development of these concepts that deserve acknowledgment. The authors would like to thank all contributors to the MANET and AUTOCONF WG efforts and those that have helped in the review and content process.

While not entirely complete the authors would like to in particular thank the following individuals for extensive discussions and valuable contributions:

Jari Arkko
12. Informative References


Authors’ Addresses

Ian D Chakeres
Motorola
Bagmane Tech Park
66/1, Plot 5, CV Raman Nagar
Bangalore, Karnataka  560093
India

Email: ian.chakeres@gmail.com
URI: http://www.ianchak.com/

Joe Macker
Naval Research Laboratory
Washington, DC  20375
USA

Email: macker@itd.nrl.navy.mil

Thomas Heide Clausen
LIX, Ecole Polytechnique
91128 Palaiseau CEDEX
France

Email: T.Clausen@computer.org
URI: http://www.thomasclausen.org/
Full Copyright Statement

Copyright (C) The IETF Trust (2007).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at http://www.ietf.org/ipr.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).