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 December 21, 2007.

Copyright Notice

Copyright (C) The IETF Trust (2007).

Abstract

This document discusses Mobile Ad hoc NETworks (MANETs). It introduces basic MANET terms, characteristics, and challenges. This document also defines several MANET entities and architectural concepts.
Table of Contents

1. Introduction .................................................... 3
2. Terminology ..................................................... 3
   2.1. Borrowed Terminology .................................... 3
   2.2. MANET Terminology ....................................... 5
3. MANET Motivation Discussion ................................. 6
4. MANET Interface Characteristics ............................ 7
   4.1. Qualities - Wireless, Mobile, Ad hoc .................. 7
   4.2. Challenges ................................................. 8
   4.2.1. Semi-Broadcast Interface ............................. 8
   4.2.2. Fuzzy Relationships Between Nearby MANET Routers &
           MANET Routers Extended Neighborhood ................. 9
   4.2.3. MANET Membership ..................................... 9
5. Addressing & the MANET Prefix Model ...................... 10
   5.1. General Address Architecture ........................... 11
   5.2. MANET Interface Configuration .......................... 12
   5.3. Routers and Hosts in a MANET ........................... 13
6. MANETs’ Place in the Network Stack ....................... 14
7. Cross Layering ................................................... 15
8. Deployment Taxonomy ............................................. 15
   8.1. Service Availability .................................... 15
   8.2. Number of MANET Routers in a MANET ................... 16
   8.3. Example Deployments .................................... 17
9. Security Considerations ....................................... 17
10. IANA Considerations .......................................... 17
11. Acknowledgments .............................................. 17
12. Informative References ...................................... 18

Authors’ Addresses ............................................... 19

Intellectual Property and Copyright Statements ............ 21
1. Introduction

A Mobile Ad hoc NETwork (MANET) consists of a loosely connected set of MANET routers. Each MANET router embodies routing/forwarding functionality and may also incorporate host functionality. These routers organize and maintain a routing structure among themselves. These routers may communicate over wireless links with asymmetric reachability, may be mobile, and may join and leave the network at any time. MANETs’ characteristics create challenges in several areas, and may require protocol extensions or new MANET protocols altogether.

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

Much of the terminology in this document was borrowed from existing documents, to list a few [RFC1812], [RFC2328], [RFC2453], [RFC2460], [RFC2461], [RFC3513], [RFC3753], [I-D.iab-multilink-subnet-issues], [I-D.templin-autoconf-dhcp], and [I-D.ietf-ipv6-2461bis]. Note that the original text for the terms is often modified, though we have attempted to maintain the same meaning.

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 communications facility at a layer below IP, over which nodes exchange IP packets directly without decrementing IP TTL (Hop Limit).
Asymmetric Reachability
A link where non-reflexive and/or non-transitive reachability is part of normal operation. Non-reflexive reachability means that packets from X reach Y but packets from Y don’t reach X. Non-transitive reachability means packets from X reach Y, and packets from Y reach Z, but packets from X don’t reach Z. Many radio/wireless interfaces exhibit these properties.

Neighbor
If node X can directly exchange IP packets with node Y, then node Y is node X’s neighbor.

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

Broadcast Interface
An interface supporting many attached nodes, together with the capability to address a single link layer transmission to all of the attached nodes (broadcast). The set of nodes receiving a given physical broadcast message are the neighbors of the node originating the message.

Full-Broadcast Interface (FBI)
A broadcast interface which does not exhibit asymmetric reachability. All nodes on the interface can send and receive IP packets directly, all nodes are symmetric neighbors. An Ethernet segment is an example of a FBI.

Semi-Broadcast Interface (SBI)
A broadcast interface that may exhibit asymmetric reachability. A FBI is a special case of SBI. Multiple access wireless radio interfaces are often SBI.

Site
A set of one or more links.

Flooding
The process of forwarding or distributing information to all devices with in a bounded region.

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

We define the following MANET entity:

MANET Router (MNR)
a MANET router embodies router functionality and may also incorporate an internally addressable host (IAH) logic, as illustrated in Figure 1. A MANET router has one or more interfaces. To simplify discussion we will classify the interfaces into two categories: classic IP interfaces & MANET interfaces. MANET interfaces are defined as interfaces that demonstrate asymmetric reachability and/or neighboring nodes with addresses that are not known a priori. A MANET router may also have zero or more classic IP interfaces to which other nodes may connect; i.e. the router may be responsible for several IP prefixes. A MANET router may participate in routing on zero or more MANET interfaces. A MANET router may participate in routing on zero or more classic IP interfaces.

---

Figure 1: MANET Router

In MANETs there are several architectural scopes. We define the following scopes:
MANET Neighbors
a set of MANET routers that is reachable via one IP hop, reachable
via link-local [RFC4007] messaging.

MANET N-Neighborhood
a set of MANET routers that is reachable via N-hops. These
routers usually have a large number of common neighboring MANET
routers and may directly compete for the same shared wireless
resources.

MANET
a routing region consisting of a set of MANET routers that is
reachable via one or more MANET router hops. If a MANET connects
to other routing regions, its border is defined by Border Routers.

If a link forms between two previously separated MANET routers or
MANETs, the two MANETs will merge to form a single larger MANET.
Similarly, if a critical link between two MANET routers is lost, then
the MANET will be partitioned into two now separate MANETs.

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

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.

The initial motivation for MANETs was called Packet Radio (PR)
networking [FL01]. In PR, each router is equipped with a single SBI.
This configuration is the simplest MANET router configuration. 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 R1 to send packets to R3, the intermediary R2 must
relay the packets. This implies that R2 must receive the packet from
R1 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 R3. This example also illustrates how
SBIs differ from FBIs: from the point of view of R2, both R1 and R3
are neighboring routers, whereas R1 and R3 are not themselves
neighboring routers of one another.
In addition to nodes’ asymmetric reachability other challenges exist. In PR networks, shared wireless resources result in interdependence between nearby nodes, and these nodes often communicate directly or indirectly. The dynamic wireless interface characteristics and node mobility often manifest as frequent network topology changes.

PR networks also lead to several other architecture related challenges. One challenge was to attach these PR networks to 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.

These PR network challenges helped stimulate the Internet Protocol; an architecture based on connectionless networking and packet-based forwarding that enables interconnection of heterogeneous devices over heterogeneous interfaces.

4. MANET Interface Characteristics

Inheriting from Packet Radio as described above, chief 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 MANET several qualities impact protocol design. The most fundamental qualities are wireless interface characteristics, mobility, and ad hoc interaction.

Wireless interfaces exhibit challenging characteristics when compared to wired interfaces. Many protocols (e.g. IPv6 neighbor discovery [RFC2461]) do not operate in wireless networks with asymmetric reachability. Wireless interfaces also exhibit time varying performance that can significantly impact local communication.
Mobility can also exacerbates wireless networking 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

MANETs 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 (with non-transitive and non-reflexive properties) and spatially distributed nodes, each node may have a different unique partial view of the MANET. That is, each node may have a different set of adjacent nodes.

Communication Range
-----------------------
Single   <--------->     <--------->
SBI      ++--          ++--
         |  R1     |  R2     |  R3     |
         ----+    ----+    ----+
          R1    R2    R3

Figure 3: Semi-Broadcast Interface (SBI) Neighboring Routers

The possibly unique set of adjacent nodes in each node often requires nodes to forward packets out the same wireless interface as the one over which they were received. Topologically, this act of forwarding out the same interface causes a packet to reach a possibly different set of nodes by traversing the wireless communication medium in a new location. An example is provided in Figure 3, where each router is capable of reaching a different set of 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 at routers with more than one neighboring router,
While also reaching a new subset of nodes.

4.2.2. Fuzzy Relationships Between Nearby MANET Routers & MANET Routers

Extended Neighborhood

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 expected interface characteristics: non-transitive, non-reflexive, time varying, and other wireless properties.

Historically, two nodes are either neighbors or not neighbors and several simple mechanisms have been used to determine a neighbor relationship: single packet reception, acceptable loss rates, and simple handshakes. In wireless networks the types of neighbor relationships expand, as do the mechanisms to detect and maintain the state of such relationships.

In wireless networks, nodes may often have non-reflexive (also often seen called unidirectional) communication links. Wireless networks also experience significant time varying packet delivery, so simple loss rates may not be sufficient to define a neighbor relationship. Similarly, as nodes move relatively to each other, past loss rates may not reflect future communication capabilities.

In wireless systems, nodes within the same small geographic region are often densely connected with other nearby nodes. These nodes form a set of extended neighbor relationships that is referred to as a neighborhood. A neighborhood is typically composed of several nodes, with each node being densely connected to other nodes.

These more dynamic neighbor relationships do not sit well with certain Internet Protocols designed assuming an fixed Ethernet like model to communication links (reflexive, transitive, and stable). Given the fuzzy neighbor relationships between MANET routers, the addressing model often associated with an Ethernet link is not valid. For example, in an Ethernet network routers are often told that a particular range of addresses are directly reachable. In MANETs’ a node often cannot make assumptions that a particular set of addressable nodes is always reachable. Instead, nodes must detect and determine neighboring devices, 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 regions. These routers are called Border Routers (BR), and they often run multiple routing protocol instances. The BR are responsible for choosing the routing information to share between the various attached routing regions. The BR should also present a consistent picture of the nodes reachable through them.

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

5. Addressing & the MANET Prefix Model

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

This architectural model considers MANET routers as simply routers with nodes attached, as illustrated in Figure 5. The attached nodes may be "external" (i.e. attached to the router via other network interfaces) or an internal addressable host logic (IAH) - however the important observation to make is, that the links between these entities and the router are classic IP links. This fact implies that, from the point of view of these entities and the applications running on them, connectivity is via a classic IP link. Therefore applications are not exposed to the specific characteristics of interfaces with asymmetric reachability or unknown address membership. Hosts are connected to the MANET via a MANET router, which has one or more interfaces participating in MANET routing.

A MANET router can be delegated zero or more prefixes. If a MANET router is delegated a prefix p::, then prefixes derived from this prefix (p:1::, p:2::, ...) may be assigned to the MANET routers interfaces towards classic IP link(s), and nodes on these classic IP links may be assigned addresses from within this prefix, and configured with this prefix according to the address autoconfiguration mechanisms governing these links [RFC2461] and [RFC2462]. This concept is illustrated in Figure 6.

Interface(s) with asymmetric reachability or unknown/indeterministic membership attached to the router are specifically *NOT* configured with this prefix. The configuration of these MANET interfaces are
If a MANET router via one of its interfaces is connected to a classic IP link, on which an existing prefix and address allocation entity is present, then this interface towards that classic IP link may be configured with addresses and prefixes from that classic IP link. This information may be in addition to or instead of configuring the MANET routers interface towards that classic IP link with a prefix derived from the prefix delegated to the MANET router. A MANET routing protocol running on the MANET routers’ MANET interface(s) may or may not include addresses and prefixes acquired on that MANET routers’ interfaces towards classic IP links in its routing messages. The routing protocol configuration is administratively determined when deploying a MANET.

<table>
<thead>
<tr>
<th>MANET Interface</th>
<th>Example Assigned Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>MANET +--------</td>
<td>=========</td>
</tr>
<tr>
<td>Router R</td>
<td>'</td>
</tr>
<tr>
<td></td>
<td>+------</td>
</tr>
<tr>
<td></td>
<td>:</td>
</tr>
<tr>
<td></td>
<td>: +-----</td>
</tr>
<tr>
<td>=Classic IP= '</td>
<td>=========</td>
</tr>
<tr>
<td>=Interfaces= :</td>
<td>=========</td>
</tr>
<tr>
<td></td>
<td>+-------</td>
</tr>
<tr>
<td></td>
<td>++--</td>
</tr>
<tr>
<td>P:2::1</td>
<td>P:2::N</td>
</tr>
</tbody>
</table>

Figure 6: MANET Router and Prefixes

5.2. MANET Interface Configuration

MANET specific behaviors are exclusively exposed to the MANET interface(s) of the routers. This behaviors may include asymmetric reachability, semi-broadcast interfaces, fuzzy MANET router neighbor relationships, unknown/indeterministic MANET membership, rapid topology dynamics, etc.
The following characteristics deserve particular mention, since they distinguish these MANET interface(s) and the MANET link model from the classic IP link model:

Unique Prefixes
MANET interfaces 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, since node membership cannot be ensured. Some common ways to achieve this are:

* unnumbered interfaces (IPv4) [RFC1812];
* link-local addresses (IPv6);
* /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 statement is 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 broadcast address reaches the interfaces of neighboring MANET routers, regardless of their configured addresses. Link-local packets are never forwarded and since a MANET may span several hops, nodes cannot assume that a packet sent to a link-local address will reach all MANET 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 router and host in a MANET, recognizing that:

- MANET interfaces are seen only by the MANET aware router, assumed to be MANET aware, and running appropriate protocols;
- nodes and subnets on non-MANET interface(s) assume a classic IP link model;
- applications on hosts and protocols assuming classic IP interfaces run unmodified.

MANET protocols are protocols which are developed to work on MANET interfaces 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 the routers over classic IP interfaces with well-known 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. The challenges discussed above, 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.

MANET MAC layer (L2) routing, more often called bridging, may work in homogeneous wireless networks for delivering frames over multiple hops. One example of L2 MANET is being developed in the IEEE 802.11s effort.

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 wired bandwidth resources are available.

L2 MANET does not enable heterogeneity. That is, 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 vary, as this could require breaking a single frame into multiple frames of a different format.

L3 MANET enables 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 higher layers. One example
is peer-to-peer (P2P) networks. These networks have some of the same challenges as MANET, e.g. variable neighbor relationships and changing membership.

7. Cross Layering

In wireless networks, and especially in MANET, extended interfacing among the network layers (physical, MAC, link, network, etc.) can be extremely useful. Arguably, for MANET deployments to be successful, some degree of cross layering 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 a 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 by itself may not be a good indicator that a node is or is not reachable.

In networks with several different layers of MANET mechanism, 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, and neighboring MANET router state changes to reduce the messaging or the latency in making decisions.

8. 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.

8.1. 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 devices. 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 intra-AS routing can be developed based upon the expected constraints and operating conditions.

8.2. Number of MANET Routers in a MANET

The number of peer MANET routers in a MANET 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 region. That is, the number of MANET routers within a single routing region.

While the number of peer MANET routers does not define scalability of a MANET protocol, it is often useful to discuss the number of peer 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 peer MANET routers

**Moderate**
- 30-100 peer MANET routers

**Large**
- 100-1000 peer MANET routers

**Very large**
- Larger than 1000 peer MANET routers

At the time of writing, small and moderate size peer MANET routing scenarios have matured and have reasonable testing and deployment experience. These sizes can perform reasonably well in many cases without hierarchy. MANET architectures can, of course, support routing hierarchies to improve scaling. Large and very large MANET routing regions that are flat are still a topic of active research and are not considered here. One can apply hierarchy to achieve scaling, but again that is not being discussed here. Existing MANET routing developments, such as SMF [I-D.ietf-manet-smf], have shown significant performance improvements and capabilities even in small peer router size deployments and experiments using classical routing designs.
8.3. Example Deployments

Here we provide a short list of example deployment scenarios:

Home, office, campus, and community mesh networks
Disaster relief and first responder networks
Sensor networks
Range extension
Military communications
Automotive networks

9. Security Considerations

TBD

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 their discussions and contributions:

Jari Akko
Emmanuel Baccelli
12. Informative References


[I-Dtemplin-autoconf-dhcp] Templin, F., "MANET Autoconfiguration",  

draft-templin-autoconf-dhcp-07 (work in progress), March 2007.


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/
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 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).