Network Working Group F. L. Templin, Ed.
Internet-Draft Boeing Technology Innovation
Intended status: Informational D. J. Jakubisin
Expires: 28 February 2026 National Security Institute, Virginia Tech
27 August 2025

MANET Internetworking: Problem Statement and Gap Analysis
draft-templin-manet-inet-00

Abstract

[RFC2501] defines a MANET as "an autonomous system of mobile nodes. The system may operate in isolation, or may have gateways to and interface with a fixed network" (such as the global public Internet). This document presents a MANET Internetworking problem statement and gap analysis.

Status of This Memo

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

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on 28 February 2026.

Copyright Notice

Copyright (c) 2025 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 (https://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. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction

Mobile Ad-hoc Networks (MANETs) [RFC2501] often include mobile nodes with limited range wireless transmission media interfaces that establish links via a dynamically changing set of neighbors within operational range. Each mobile node engages a MANET routing protocol to discover links to first hop neighbors as well as multihop paths to reach other nodes beyond. As IP routers [RFC0791][RFC8200], MANET routers represent multihop paths as "host routes" established through either proactive or reactive discovery.

Individual MANETs typically include modest numbers of mobile nodes (e.g., O(1), O(10), O(100), etc.) which naturally limits the number of host routes needed in the local routing system. MANETs can merge to form larger MANETs and/or partition into smaller MANETs according to dynamic network conditions such as mobility. MANETs often operate autonomously unless or until they encounter Internetwork access points of opportunity.

Data communications between two nodes within the same MANET follow host routes using MANET-internal links. When a MANET router establishes an Internetwork link, it can provide "Internet connection-sharing" access to the rest of the MANET as a connected "stub" network. Per [RFC2501], "stub networks carry traffic originating at and/or destined for internal nodes, but do not permit exogenous traffic to "transit" through the stub network".

Practical applications however suggest that MANETs can act as true stub networks (e.g., a cellphone that provides a hotspot for a multihop WiFi SSID) or as "not-so-stubby" networks (e.g., Intelligent Transportation Systems where the 5G/6G "SideLink" service supports vehicle-to-vehicle (V2V) multihopping). In the former case, the cellphone acts as an IP router for a stub WiFi MANET behind it and the multihop WiFi nodes act as dependent nodes. In the latter case, individual 5G/6G SideLink nodes can connect the stub MANETs they aggregate across not-so-stubby V2V multihop forwarding paths. MANET Internetworking must therefore be capable of accommodating all such scenarios.

Google AI reports that: "There are currently more mobile phones than people in the world. While the exact number fluctuates, estimates suggest there are over 12 billion mobile connections worldwide". Each mobile node that connects to the global public Internet can therefore be regarded as a network access point for a singleton "MANET" with the potential to connect still larger MANETs.

2. MANET Internetworking Problem Statement and Gap Analysis

2.1. Problem 1: MANET Local Addressing

Each MANET router requires a unique IP address for MANET-local communications; the router often uses this same address to configure a unique "router ID". For MANETs that are only intermittently connected to an Internetwork, these addresses must be generated from IP prefixes of scope greater than link-local but not associated with infrastructure aggregation points. For all MANET types, each address/ID must be locally-unique within the (limited) local MANET routing domain. For not-so-stubby MANETs, the address/ID must also be globally-unique among all local MANET routing domains worldwide.

The locally-unique property ensures that no two nodes that participate in the MANET routing protocol within the same local routing domain configure the same address/ID. The globally-unique property may seem moot until one considers that MANETs can merge with other MANETS, and nodes from a first MANET can freely move to other MANETs. This may allow a node from a first MANET where there are no duplicates to encounter other MANETs where a duplicate address may be encountered.

Although the node population for each MANET local routing domain is likely to be modest, the total population of MANET nodes may be on the order of the number of worldwide mobile connections (12B). Therefore, if MANET nodes assigned random addresses from a 64-bit space, the probability of one or more collisions within the total world population (i.e., when multiple nodes independently configure the same address) exceeds 98% [RFC9374]. With such a high likelihood of duplication for some pair(s) of nodes in the world population, an unresolvable collision would occur if duplicates ever met within the same local routing domain.

For stub MANETs that always acts independently of all others, the risk of a duplication event within each local routing domain due to a new node joining is vanishingly small even for extreme mobility frequencies according to Appendix A.2 of [RFC4429]. Stub MANETs can therefore rely on statistical uniqueness properties of randomly assigned addresses.

When MANET Internetworking is applied for connecting routers in different not-so-stubby MANETs, however, independent local routing domains are dynamically joined by (temporary) switched virtual circuits across the Internetwork overlay as a normal course of operational data communications. When these temporary MANET merge events occur, the MANET local IP addresses present in the source and destination MANETs must be mutually exclusive. These merge events must further be considered to occur at truly unbounded frequencies across the global population due to the unpredictable nature of worldwide Internetworking dynamics for peer-to-peer communications. Statistical uniqueness properties of random assignments from even very large populations may therefore be insufficient to ensure collision freedom.

MANET Internetworking therefore regards the global public Internet as a "MANET-of-MANETs", and with unbounded dynamic relationships between distinct local MANET routing regions joined by switched virtual circuits. This exposes the full world population of MANET local addresses as potential duplicates.

Nodes in not-so-stubby MANETs should therefore configure MANET local addresses managed for uniqueness even if they first self-generate the addresses before enrolling them in a registration service. Such address registration is not required for nodes that only connect via stub MANETs.

2.2. Problem 2: Autoconfiguration

When a MANET comes in contact with a fixed Internetwork such as the global public Internet, nodes in the MANET that engage global mobile Internetworking services require some means of autoconfiguring global-scoped IP addresses and/or prefixes that are properly routable by network elements accessible from the current point of attachment. These network elements are typically proxies or routers of some variety that connect to the mobile routing system.

Nodes in the local MANET that are multiple IP hops away from an Internet connection sharing peer cannot use unmodified standard autoconfiguration services including IPv6 Neighbor Discovery (IPv6ND) [RFC4861] or DHCPv6 [RFC8415] over a MANET interface since these services are link-scoped in nature. (The DHCPv6 architecture includes a "relay" function, but the dynamic nature of links in (multi-link) local MANET routing regions precludes straightforward application of DHCPv6 relays.)

Two methods of supporting generalized autoconfiguration for nodes within a MANET have been suggested. In a first method (conducted directly over MANET interfaces) first-hop neighboring nodes within the MANET collectively participate to repeat link-scoped autoconfiguration discovery requests to other neighbors that are topologically closer to an Internet connection sharing node. This hop-by-hop process continues between neighbors until the request arrives at an Internet connection sharing node that can then contact an Internetwork element capable of delegating an Internet Service Provider (ISP) Provider-Aggregated (PA) IP address or prefix. The Internetwork element then returns the delegated IP address/prefix in a reply that traverses the reverse path to the original requesting node. Each MANET router then configures a route to this IP address/prefix within the MANET local routing protocol, i.e., the MANET local routing protocol is made aware of the delegation.

In a second autoconfiguration method, the requesting node configures a (virtual) overlay multilink network interface over its (physical) MANET interface(s) and issues standard link-scoped IPv6ND and/or DHCPv6 requests over the virtual interface. The virtual interface applies encapsulation to provide the appearance of a single Non-Broadcast Multiple Access (NBMA) link spanning the entire (multilink) MANET. This virtual link supports standard link-scoped autoconfiguration services coordinated with an Internetwork element capable of delegating an address. For stub MANETs, the Internet connection sharing node itself delegates a public or private IP address. For not-so-stubby MANETS, an overlay network element beyond the Internet connection sharing node delegates a Mobility Service Provider (MSP) Proxy-Aggregated (PA) and/or Proxy-Independent (PI) IP address/prefix as overlay network addresses. The delegating node then returns the delegated IP address/prefix in a link-scoped reply over the virtual interface that traverses the reverse path to the original requesting node. Each MANET router optionally configures a route to this IP address/prefix via the virtual interface, i.e., the MANET local routing protocol is optionally made aware of the delegation within the virtual overlay.

2.3. Problem 3: MANET-internal Communications

Two nodes located within the same local MANET routing region should be able to communicate (across multiple hops if necessary) using MANET local addressing with no external Internetwork infrastructure reference points. As long as the MANET-local addresses configured by communicating peers are unique, the MANET local routing system maintains continuous multihop forwarding services to ensure session continuity.

Nodes within the local MANET routing region can discover the MANET local addresses of peers using services like Multicast DNS (mDNS) [RFC6762] supported by Simplified Multicast Forwarding (SMF) [RFC6621]. Peer-to-peer communications can then be coordinated either in multihop fashion directly over the physical MANET interfaces or via a single virtual hop using overlay multilink network interface encapsulation. In that case, the MANET peers establish a switched virtual circuit spanning any intermediate hops in the path.

2.4. Problem 4: MANET Peer to Internetwork Correspondent

When an originating peer (or its stub MANET Internet connection-sharing node) within a not-so-stubby MANET needs to communicate with a correspondent connected elsewhere in an external Internetwork, the peer consults the global DNS which returns a (stable) globally-routable IP address for the correspondent. The peer can then use one of its MSP-provided PA/PI IP addresses obtained through autoconfiguration and the global IP address of the Internetwork correspondent as the source and destination addresses for packet exchanges.

The MANET peer first establishes a switched virtual circuit in the overlay to an Internetwork relay beyond the MANET border. MANET local multihop routing will then convey the peer's original packets to the Internetwork relay which engages standard Internetwork routing and forwarding to direct the packets to the correspondent node. In the reverse path, the correspondent uses the overlay IP address of the peer obtained from the source address of initiating packets as the destination address for reply packets. Standard Internetwork routing will direct the packets back to the relay which then forwards them via an overlay switched virtual circuit to the originating peer's MANET border. MANET-local routing and forwarding will then convey the packets over one or more MANET-local hops until they ultimately reach the peer.

In this case, the originating peer's IP address need not appear in the global DNS since the correspondent discovers the address by examining the source of received packets. This means that the originating peer can use a PA address to initiate sessions. However, if the PA address changes (e.g., due to movement to a new Internetwork attachment point) any communication sessions in progress with Internetwork correspondents will fail and the peer will need to re-establish them under the new PA address.

2.5. Problem 5: Internetwork Correspondent to MANET Peer

When an Internetwork correspondent needs to communicate with a target peer within a local MANET routing region, the correspondent consults the global DNS. Due to the uncertainty of mobility-based re-addressing for PA addresses, however, the peer would be best served by including only PI addresses in its global DNS resource records.

The correspondent then forwards packets via standard Internet routing until they arrive at a relay. The relay then establishes a switched virtual circuit in the overlay to the MANET peer then begins forwarding packets via the switched virtual circuit until they reach the destination.

PI addresses remain stable even across MANET-wide mobility events to the point that continuous dynamic updates to the DNS would not be necessary to maintain uninterruptable communications. While it is possible that mobility events may cause minor temporary disruptions, transport protocol retransmissions will maintain continuity for any ongoing sessions.

2.6. Problem 6: Peer-to-Peer Between Different MANETs

When two prospective peer nodes are located in different MANET local routing regions with a common Internetwork as a transit network, both peers should include PI addresses in their global DNS resource records for the same reasons cited in Section 2.5.

The peers then establish switched virtual circuits in the overlay to support peer-to-peer bidirectional packet forwarding.

Maintaining PI addresses requires a certain degree of coordination between peer nodes and the MSP. The MSP is responsible for ensuring that each peer remains reachable at its stable PI address/prefix through distributed mobility management.

2.7. Problem 7: Stub MANET to Not-so-stubby MANET Connections

When an Internet connection sharing MANET router connects a stub MANET, it can either delegate true PI addresses to stub MANET nodes or delegate private IP addresses then apply Network Address Translation (NAT) to support external communications.

In the PI case, all manners of peer-to-peer communications are made possible due to the globally routable nature of PI addresses. In the NAT case, only communications initiated by a stub network peer are supported since the reverse path terminates at the NAT.

The stub MANET itself may configure a local overlay that regards the (multihop) MANET as a single unified link. In that case, the stub network overlay link is distinct from the overlay link that spans the global public Internet and the two links are joined by an IPv6 router.

3. IANA Considerations

This document is an informational problem statement and does not in itself request any IANA actions. IANA considerations can be found in solution space document.

4. Security Considerations

This document is an informational problem statement and does not in itself address security. Security considerations can be found in solution space document.

5. Acknowledgements

Discussions on the MANET working group mailing list helped shape concepts exposed in this document.

This work is aligned with the Boeing/Virginia Tech National Security Institute (VTNSI) 5G MANET research program.

Honoring life, liberty and the pursuit of happiness.

6. References

6.1. Normative References

[RFC0791] Postel, J., "Internet Protocol", STD 5, RFC 791, DOI 10.17487/RFC0791, September 1981, <https://www.rfc-editor.org/info/rfc791>.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017, <https://www.rfc-editor.org/info/rfc8200>.

6.2. Informative References

[RFC2501] Corson, S. and J. Macker, "Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations", RFC 2501, DOI 10.17487/RFC2501, January 1999, <https://www.rfc-editor.org/info/rfc2501>.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006, <https://www.rfc-editor.org/info/rfc4429>.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007, <https://www.rfc-editor.org/info/rfc4861>.

[RFC6621] Macker, J., Ed., "Simplified Multicast Forwarding", RFC 6621, DOI 10.17487/RFC6621, May 2012, <https://www.rfc-editor.org/info/rfc6621>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013, <https://www.rfc-editor.org/info/rfc6762>.

[RFC8415] Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., Lemon, T., and T. Winters, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 8415, DOI 10.17487/RFC8415, November 2018, <https://www.rfc-editor.org/info/rfc8415>.

[RFC9374] Moskowitz, R., Card, S., Wiethuechter, A., and A. Gurtov, "DRIP Entity Tag (DET) for Unmanned Aircraft System Remote ID (UAS RID)", RFC 9374, DOI 10.17487/RFC9374, March 2023, <https://www.rfc-editor.org/info/rfc9374>.

Appendix A. Change Log

<< RFC Editor - remove prior to publication >>

Differences from earlier versions:

* First draft publication.

Authors' Addresses

Fred L. Templin (editor)
Boeing Technology Innovation
P.O. Box 3707
Seattle, WA 98124
United States of America
Email: fltemplin@acm.org

Daniel J. Jakubisin
National Security Institute, Virginia Tech
2202 Kraft Dr.
Blacksburg, VA 24060
United States of America
Email: djj@vt.edu