Network Working Group   F. L. Templin, Ed.
Internet-Draft   Boeing Technology Innovation
Intended status: Informational   D. J. Jakubisin
Expires: 9 August 2026   National Security Institute, Virginia Tech
5 February 2026

MANET Internetworking with AERO/OMNI
draft-templin-manet-inet-omni-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 framework based on the Automatic Extended Route Optimization (AERO) and Overlay Multilink Network (OMNI) Interface technologies.

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.); this 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 may also have internal clusters with cluster heads that limit the extent over which host routes propagate to reduce control message overhead. Finally, MANETs often operate autonomously unless or until they encounter Internetwork access points of opportunity.

Data communications between two nodes within the same local MANET routing region 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 either true stub networks (e.g., a cellphone providing 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 individual 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 in some sense be regarded as a network access point for a singleton "MANET" with the potential to connect still larger MANETs.

MANET Internetworking therefore regards the global Internet as a "network of (mobile ad-hoc) networks", and with unrestricted dynamic relationships between distinct local MANET routing regions joined by virtual circuits. Figure 1 illustrates an example of two distinct MANETs joined by a virtual circuit using the Global Internet as transit:

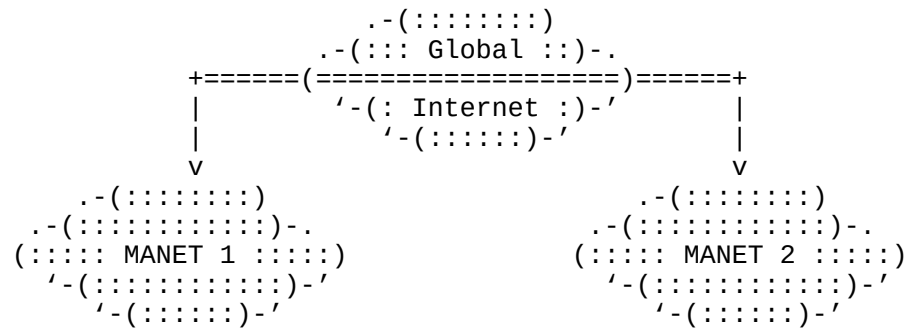

Figure 1: MANET Internetworking

In this context, a number of gaps have been identified to bring robust MANET Internetworking to fruition [I-D.templin-manet-inet]. The purpose of the present submission is to describe approaches to addressing these gaps based on the Automatic Extended Route Optimization (AERO) [I-D.templin-6man-aero3] and Overlay Multilink Network (OMNI) Interface [I-D.templin-6man-omni3] solutions.

2. MANET Use Cases

MANETs have an important role in emergency response communications, disaster relief situations, communications in remote and rural areas, military operations, vehicular and swarm communications, and low-powered Internet of things (IoT) applications. MANETs provide the ability to establish and maintain communications when infrastructure-based networks, such as 5G cellular communication systems, are not accessible. As described above, MANETs may also provide Internet connectivity to internal nodes, for example, as a "stub" network via MANET routers which possess an Internetworking capability and an external connection to a radio access network.

Example use cases of such MANETs include the following:

* Disaster Relief: Disaster situations may compromise network infrastructure, such as through the loss of base stations in a cellular radio access network (RAN). In this scenario, MANET networks can play a role in closing coverage gaps through multi-hop routing to nodes within the coverage area of uncompromised base stations. This use case is broadly applicable to any situation in which nodes are operating outside or at the periphery of RAN coverage.

* Tracking and Monitoring: Another example use case is the tracking and monitoring of data from low-cost low-power IoT devices ("tags") which may be placed on packages during shipment or

storage. Such devices may transition in and out of coverage of infrastructure-based networks, often being located in environments that are not conducive to RF propagation (e.g., shipping container, warehouse, etc.). The ability to discover and connect to neighboring MANET-enabled devices and to establish Internet connectivity through such MANETs, enables real-time logistics and inventory data to be collected opportunistically.

* UAV Swarms: local communications within swarms for coordination and cooperation is a good use case for MANET networks due to the highly mobile dynamic nature of such networks. Yet swarms may also benefit from connectivity to the Internet, or other external networks. And in large swarm-based MANETs, routing of traffic through infrastructure networks to MANET endpoints, rather than traversing the entire MANET can improve communications throughput and reliability.

3. MANET Internetworking with AERO/OMNI

3.1. 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 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 interact with other MANETs where a duplicate address may be encountered resulting in unpredictable behavior and/or communication failures.

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 (see: Section 1). Assuming the google estimate of O(10**10) wireless connections, 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 in the worldwide population, an unresolvable collision could occur if duplicates ever met within the same local routing domain (e.g., following a MANET merge).

When MANET Internetworking is applied to connect routers in different not-so-stubby MANETs, independent local routing domains are dynamically joined by on-demand virtual circuits across an Internetwork overlay as a normal course of operational data communications. When these 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 since MANET Internetworking 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 global uniqueness even if they first self-generate the addresses before enrolling them in a registration service. The IPv6 Multilink Local Address (MLA) provides a suitable solution for this purpose [I-D.templin-6man-mla].

3.2. MANET 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 or prefixes that are properly routable by network elements accessible from the current point of attachment. These network elements are typically proxies or gateways 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 may interfere with straightforward application of DHCPv6 relays.)

To engage in autoconfiguration, 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 IP prefixes. The Overlay Multilink Network (OMNI) Interface specification [I-D.templin-6man-omni3] and its companion Automatic Extended Route Optimization (AERO) [I-D.templin-6man-aero3] were designed for this purpose.

All MANET nodes as well as AERO/OMNI Internetwork Proxy/Servers and Gateways assign a unique MLA to their OMNI virtual interface. An AERO/OMNI Mobility Anchor Point (MAP) delegates a Mobility Service Provider (MSP) Mobile Network Prefix (MNP) as a Provider-Independent (PI) IP prefix maintained by the overlay for the requesting node to provision on downstream-attached interfaces in the manner discussed in [RFC9663] and [RFC9762]. The MAP then returns the delegated MNP in a link-scoped reply over the OMNI interface that traverses the reverse path to the original requesting node.

The MLAs assigned as described above are routable within an OMNI link limited domain [RFC8799], but are generally not otherwise routable to destinations in other domains. MANET nodes therefore also obtain globally routable IP MNPs from supporting MAP Proxy/Servers to support global-scoped communications; address selection policies should prefer these MNP-based addresses when available since MLAs are only routable within a limited domain.

3.3. MANET-internal Communications

Two nodes located within the same local MANET routing region should be able to communicate (across multiple hops if necessary) using MLA addressing with no external Internetwork infrastructure reference points. As long as the MLAs 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 MLAs and/or MNP-based global addresses of peers using Multicast DNS (mDNS) [RFC6762] supported by Simplified Multicast Forwarding (SMF) [RFC6621]. Peer-to-peer communications can then be coordinated in multihop fashion using OMNI encapsulation and header compression over on-demand virtual circuits spanning any MANET intermediate hops in the path.

3.4. 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 MNP-based 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 an on-demand 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 MANET border which then forwards them via the overlay to an Internetwork relay which directs the packets to the correspondent node.

In the reverse path, the correspondent uses the MNP-based 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 on-demand overlay 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.

3.5. 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 to determine an IP address for the peer.

The correspondent then forwards packets via standard Internet routing until they arrive at a relay. The relay then establishes an on-demand virtual circuit in the overlay to the MANET peer then begins forwarding packets via the virtual circuit until they reach the destination. Reverse path forwarding from the MANET peer to the Internetwork correspondent is then conducted in the same manner described in Section 3.4.

IP addresses covered by delegated prefixes remain stable even across MANET-wide mobility events to the point that continuous dynamic updates to the DNS are not required 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.

3.6. Peer-to-Peer Between Different MANETs

When two prospective peer nodes are located in different MANET local routing regions separated by one or more transit Internetwork segments, both peers should include their IP addresses in their global DNS resource records for the same reasons cited in Section 3.5.

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

A certain degree of coordination between peer nodes and the MSP is the required to maintain address mappings. The MSP is responsible for ensuring that each peer remains reachable at its stable IP address/prefix through distributed mobility management.

3.7. Stub MANET to Not-so-stubby MANET Connections

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

In the public case, all manners of peer-to-peer communications are made possible due to the globally routable nature of the 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.

In the not-so-stubby case, a single overlay link extends across both any transit Internetworks and the source and target MANETs themselves. All peer-to-peer communications are therefore conveyed across the monolithic Internetwork overlay.

4. IANA Considerations

This document is informational and does not in itself request any IANA actions. IANA considerations can be found in the solution space documents cited.

5. Security Considerations

This document is informational and does not in itself address security. Security considerations can be found in the solution space documents cited.

6. Acknowledgements

This work is derived directly from "MANET Internetworking: Problem Statement and Gap Analysis" [I-D.templin-manet-inet].

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.

7. References

7.1. 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>.

7.2. Informative References

[I-D.templin-6man-aero3] Templin, F., "Automatic Extended Route Optimization (AERO)", Work in Progress, Internet-Draft, draft-templin-6man-aero3-52, 23 January 2026, <https://datatracker.ietf.org/doc/html/draft-templin-6man-aero3-52>.

[I-D.templin-6man-mla] Templin, F., "IPv6 Addresses for Ad Hoc Networks", Work in Progress, Internet-Draft, draft-templin-6man-mla-30, 11 November 2025, <https://datatracker.ietf.org/doc/html/draft-templin-6man-mla-30>.

[I-D.templin-6man-omni3]
Templin, F., "Transmission of IP Packets over Overlay Multilink Network (OMNI) Interfaces", Work in Progress, Internet-Draft, draft-templin-6man-omni3-71, 2 February 2026, <https://datatracker.ietf.org/doc/html/draft-templin-6man-omni3-71>.

[I-D.templin-manet-inet]
Templin, F. and D. J. Jakubisin, "MANET Internetworking: Problem Statement and Gap Analysis", Work in Progress, Internet-Draft, draft-templin-manet-inet-02, 12 January 2026, <https://datatracker.ietf.org/doc/html/draft-templin-manet-inet-02>.

[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>.

[RFC8799] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <https://www.rfc-editor.org/info/rfc8799>.

[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>.

[RFC9663] Colitti, L., Linkova, J., Ed., and X. Ma, Ed., "Using DHCPv6 Prefix Delegation (DHCPv6-PD) to Allocate Unique IPv6 Prefixes per Client in Large Broadcast Networks", RFC 9663, DOI 10.17487/RFC9663, October 2024, <https://www.rfc-editor.org/info/rfc9663>.

[RFC9762] Colitti, L., Linkova, J., Ma, X., Ed., and D. Lamparter, "Using Router Advertisements to Signal the Availability of DHCPv6 Prefix Delegation to Clients", RFC 9762, DOI 10.17487/RFC9762, June 2025, <https://www.rfc-editor.org/info/rfc9762>.

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