Internet Engineering Task Force (IETF)
Request for Comments: 7137
Updates: 5820
Category: Experimental
ISSN: 2070-1721

A. Retana
S. Ratliff
Cisco Systems, Inc.

February 2014

Use of the OSPF-MANET Interface in Single-Hop Broadcast Networks

Abstract

This document describes the use of the OSPF-MANET interface in single-hop broadcast networks. It includes a mechanism to dynamically determine the presence of such a network and specific operational considerations due to its nature.

This document updates RFC 5820.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for examination, experimental implementation, and evaluation.

This document defines an Experimental Protocol for the Internet community. This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc7137.

Table of Contents

1. Introduction

The OSPF-MANET interface [RFC5820] uses the point-to-multipoint adjacency model over a broadcast media to allow the following:

- All router-to-router connections are treated as if they were point-to-point links.
- The link metric can be set on a per-neighbor basis.
- Broadcast and multicast can be accomplished through the Layer 2 broadcast capabilities of the media.

It is clear that the characteristics of the MANET interface can also be beneficial in other types of network deployments -- specifically, in single-hop broadcast capable networks that may have a different cost associated with any pair of nodes.

This document updates [RFC5820] by describing the use of the MANET interface in single-hop broadcast networks; this consists of its simplified operation by not requiring the use of overlapping relays as well as introducing a new heuristic for smart peering using the Router Priority.

1.1. Single-Hop Broadcast Networks

The OSPF extensions for MANETs assume the ad hoc formation of a network over bandwidth-constrained wireless links, where packets may traverse several intermediate nodes before reaching their destination (multi-hop paths on the interface). By contrast, a single-hop broadcast network (as considered in this document) is one that is structured in such a way that all the nodes in it are directly connected to each other. An Ethernet interface is a good example of the connectivity model.

Furthermore, the single-hop networks considered may have different link metrics associated to the connectivity between a specific pair of neighbors. The OSPF broadcast model [RFC2328] can’t accurately describe these differences. A point-to-multipoint description is more appropriate given that each node can reach every other node directly.

In summary, the single-hop broadcast interfaces considered in this document have the following characteristics:

- direct connectivity between all the nodes
- different link metrics that may exist per-neighbor
- broadcast/multicast capabilities

2. Requirements Language

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

3. Single-Hop Network Operation

The operation of the MANET interface doesn't change when implemented on a single-hop broadcast interface. However, the operation of some of the proposed enhancements can be simplified. Explicitly, the Overlapping Relay Discovery Process SHOULD NOT be executed, and the A-bit SHOULD NOT be set by any of the nodes, so that the result is an empty set of Active Overlapping Relays.

This document describes the use of already defined mechanisms and requires no additional on-the-wire changes.

3.1. Use of Router Priority

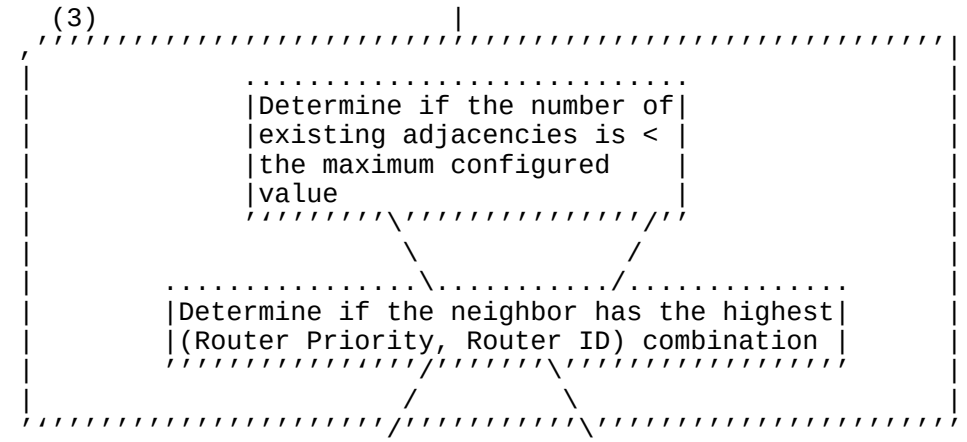
Smart peering [RFC5820] can be used to reduce the burden of requiring a full mesh of adjacencies. In short, a new adjacency is not required if reachability to the node is already available through the existing shortest path tree (SPT). In general, the reachability is verified on a first-come-first-served basis; i.e., in a typical network, the neighbors with which a FULL adjacency is set up depend on the order of discovery.

The state machine for smart peering allows for the definition of heuristics, beyond the SPT reachability, to decide whether or not it considers a new adjacency to be of value. This section describes one such heuristic to be used in Step (3) of the state machine, in place of the original one in Section 3.5.3.2 of [RFC5820].

The Router Priority (as defined in OSPFv2 [RFC2328] and OSPFv3 [RFC5340]) is used in the election of the (Backup) Designated Router, and can be configured only in broadcast and Non-Broadcast Multi-Access (NBMA) interfaces. The MANET interface is a broadcast interface using the point-to-multipoint adjacency model; this means that no (Backup) Designated Router is elected. For its use with the MANET interface, the Router Priority is defined as:

Router Priority
: An 8-bit unsigned integer. Used to determine the precedence of which router(s) to establish a FULL adjacency with during the Smart Peering selection process. When more than one router attached to a network is present, the one with the highest Router Priority takes precedence. If there is still a tie, the router with the highest Router ID takes precedence.

The heuristic for the state machine for smart peering is described as:



Smart Peering Algorithm

In order to avoid churn in the selection and establishment of the adjacencies, every router SHOULD wait until the ModeChange timer (Section 4) expires before running the state machine for smart peering. Note that this wait should cause the selection process to consider all the nodes on the link, instead of being triggered based on receiving a Hello message from a potential neighbor. The nodes selected using this process are referred to simply as "smart peers".

It is RECOMMENDED that the maximum number of adjacencies be set to 2.

3.2. Unsynchronized Adjacencies

An unsynchronized adjacency [RFC5820] is one for which the database synchronization is postponed, but that is announced as FULL because SPT reachability can be proven. A single-hop broadcast network has a connectivity model in which all the nodes are directly connected to each other. This connectivity results in a simplified reachability check through the SPT: the adjacency to a specific peer MUST be advertised as FULL by at least one smart peer.

The single-hop nature of the interface allows then the advertisement of the reachable adjacencies as FULL without additional signaling. Flooding SHOULD be enabled for all the unsynchronized adjacencies to take advantage of the broadcast nature of the media. As a result, all the nodes in the interface will be able to use all the LSAs received.

4. Single-Hop Network Detection

A single-hop network is one in which all the nodes are directly connected. Detection of such an interface can be easily done at every node by comparing the speaker's 1-hop neighbors with its 2-hop neighborhood. If for every 1-hop neighbor, the set of 2-hop neighbors contains the whole set of the remaining 1-hop neighbors, then the interface is a single-hop network; this condition is called the Single-Hop Condition.

A new field is introduced in the MANET interface data structure. The name of the field is SingleHop, and it is a flag indicating whether the interface is operating in single-hop mode (as described in Section 3). The SingleHop flag is set when the node meets the Single-Hop Condition on the interface. If the Single-Hop Condition is no longer met, then the SingleHop flag MUST be cleared.

A new timer is introduced to guide the transition of the interface from/to multi-hop mode (which is the default mode described in [RFC5820]) to/from single-hop mode:

- ModeChange: Every time a node changes the state of the SingleHop flag for the interface, the corresponding ModeChange timer MUST be set. The ModeChange timer represents the length of time in seconds that an interface SHOULD wait before changing between multi-hop and single-hop modes. It is RECOMMENDED that this timer be set to Wait Time [RFC2328].

The following sections describe the steps to be taken to transition between interface modes.

4.1. Transition from Multi-Hop to Single-Hop Mode

Detection of the Single-Hop Condition triggers the transition into single-hop mode by setting both the SingleHop flag and the ModeChange timer.

Once the ModeChange timer expires, the heuristic defined in Section 3.1 MAY be executed to optimize the set of adjacencies on the interface. Note that an adjacency MUST NOT transition from FULL to 2-Way unless the simplified reachability check (Section 3.2) can be verified.

4.2. Transition from Single-Hop to Multi-Hop Mode

Not meeting the Single-Hop Condition triggers the transition into multi-hop mode by clearing the SingleHop flag and setting the ModeChange timer. The A-bit MUST be set if the Single-Hop condition is no longer met because of one of the following cases:

- an increase in the set of 1-hop neighbors, without the corresponding increase of the 2-hop neighborhood
- a decrease of the 2-hop neighborhood while maintaining all the previous 1-hop neighbors

Once the ModeChange timer expires, the multi-hop operation described in [RFC5820] takes over.

Note that the cases listed above may result in the interface either gaining or losing a node before the ModeChange timer expires. In both cases, the heuristic defined in Section 3.1 MAY be executed to optimize the set of adjacencies on the interface.

In the case that a node joins the interface, the Designated Router and Backup Designated Router fields in the Hello packet [RFC2328] MAY be used to inform the new node of the identity (Router ID) of the current smart peers (and avoid the optimization).

5. Security Considerations

No new security concerns beyond the ones expressed in [RFC5820] are introduced in this document.

6. Acknowledgements

The authors would like to thank Anton Smirnov, Jeffrey Zhang, Alia Atlas, Juan Antonio Cordero, Richard Ogier, and Christer Holmberg for their comments.

7. References

7.1. Normative References

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

[RFC2328] Moy, J., "OSPF Version 2", STD 54, RFC 2328, April 1998.

[RFC5820] Roy, A. and M. Chandra, "Extensions to OSPF to Support Mobile Ad Hoc Networking", RFC 5820, March 2010.

7.2. Informative References

[RFC5340] Coltun, R., Ferguson, D., Moy, J., and A. Lindem, "OSPF for IPv6", RFC 5340, July 2008.

Authors' Addresses

Alvaro Retana
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
USA

EMail: aretana@cisco.com

Stan Ratliff
Cisco Systems, Inc.
7025 Kit Creek Rd.
Research Triangle Park, NC 27709
USA

EMail: sratliff@cisco.com