homenet L. Howard
Internet-Draft Time Warner Cable
Intended status: Informational December 29, 2011
Expires: July 1, 2012

Evaluation of Proposed Homenet Routing Solutions
draft-howard-homenet-routing-comparison-00

Abstract

This document evaluates the various proposals for routing in an unmanaged home network.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document evaluates the suitability of each of the proposed routing solutions for the Homenet problem space. The list of requirements is provided in [draft-howard-homenet-routing-requirements] (soon to be included in [draft-ietf-homenet-arch]). This document is intended to assist the working group in developing consensus around a single solution, so that work may progress.

2. Requirements

This section includes the requirements from [draft-howard-homenet-routing-requirements]. After each requirement is a short mnemonic, to be used in the table comparing each solution.

1. Reachability between all nodes in the home network. Links may be Ethernet, WiFi, MoCA, or any other; test all solutions against mutliple L2 types. [1. Reachability]

2. Border detection. Any solution will have to determine the routing boundary. It is assumed that no home networking device can handle a full routing table for the Internet, and that a home router should not be required to do so. [2. Border detection]

   A. Border may be upstream ISP, or may be a device that is a gateway to SmartGrid devices, e.g. a controller that speaks RPL to 802.15.4 and foo to home net. Or there may be no border, if no external connection has been established. [2a. Any border]

   B. Must be able to find "up" (a path to the Internet), but must not be dependent on "up" (Internet connectivity) existing for intra-home reachability. [2b. Find "up"]

   C. May be discovered by routing protocol, or other means. [2c. Border method]

3. Robust to routers being moved/added/removed/renumbered. Convergence time a few minutes or less. [3. Handles change]

4. No configuration required. It may be acceptable to require a single password or passphrase to be entered on each device, both for security, and to establish the administrative boundary. [4. No config]

5. Best-path is a non-requirement. [5. Null requirement]

6. Support for multiple upstream networks is a requirement. [6. Multiple upstreams]

   A. Including wireless offload, video-only, and split-tunnel VPN scenarios. [6a. Split up views]

   B. It may be assumed that each upstream will be connected via a separate router, not multihomed off the same router. [6b. Null requirement]

   C. Must support a prefix delegated from each provider. How hosts handle multiple prefixes is not a routing problem. [6c. Multiple PD]

   D. Load-balancing among providers is a non-requirement. [6d. Null requirement]

   E. If multiple upstream networks can provide a path to the same destination (such as an Internet host), the solution must allow for backup in case the router or link to one upstream fails. Failover time should be within a few minutes. [6e. Failover]

   F. Must support a "walled-garden" network. This might routing based on either source address (from the walled garden network) or destination address (to the walled garden network); support for both is not required. [6f. Walled garden]

   G. Source address selection is out of scope for the routing solution. Choosing which address to use to look up the destination address is out of scope for the routing solution. [6g. Null requirement]

7. Cannot assume hierarchical prefix delegation in the home, unless the Homenet working group finds consensus on a hierarchical addressing mechanism. [7. Non-hierarchical]

8. A host with mutliple upstream paths to the same destination (in-home or external) should be able to use another in case on fails. [8. Failover]

9. Prevent looping. [9. Prevent loops]

10. Should be a lightweight solution. [10. Lightweight]

11. Must handle multi-dwelling units or other potential dense wireless or wired networks. [11. Robust to MDUs]

12. Must be resilient to running on wireless networks. Must be able to handle both wired and wireless links. [12. Wireless]

13. Robustness in the face of unintentional joining of networks. [12. Unintended joins]

3. Consideration

3.1. OSPFv3

As documented in [OSPFv3-autoconfig].

1. Reachability. YES, OSPF can detect reachability.

2. Border detection. NO. Any node which the router uses as a next hop, but which is not in its OSPF Area 0, may be assumed to be an external border. However, the router will have to be manually configured, or use another routing protocol, to establish a path to that next hop; therefore auto-configured OSPFv3 by itself does not detect borders.

   A. Any border. NO.

   B. Find "up". NO. Manual configuration of the router neighboring the ISP is required to set a default route.

   C. Border method. MANUAL.

3. Handles change. YES. OSPFv3 normally handles router additions and removals well, with link-state changes. It may not be able to handle being moved from one existing segment to another.

4. No config. YES, but requires manual configuration for security.

5. (null)

6. Multiple upstreams. YES, OSPFv3 can support multiple default routes, and multiple specific routes.

   A. Split up views. SOMEWHAT. OSPFv3 can certainly carry many paths, including specific routes for a wireles home agent, video cluster, or VPN concentrator. It cannot, by itself, establish routing policies determining which hosts may use those paths, so the upstream ISP may not have a return path

(or may have an asymmetric path).

B. (null)

C. Multiple PD. YES, OSPFv3 can route for multiple prefixes on a link.

D. (null)

E. Failover. YES, autoconfigured OSPFv3 detects link state change and reconverges in a reasonable amount of time.

F. Walled garden. SOMEWHAT. OSPFv3 can carry destination routes, but cannot by itself support source-based routing.

G. (null)

7. Non-hierarchical addressing. YES.

8. Failover. YES.

9. Prevent loops. YES.

10. Lightweight. NO. One estimate of a common implementation is 50,000 lines of code.

11. Robust to MDUs. YES. Full LSAs are sent periodically, but they are not onerus.

12. Wireless. YES.

13. Unintended joins. NO. Autoconfig OSPFv3 is not resilient against unintended joins unless the recommendation to use authentication hashes [OSPFV3-AUTH-TRAILER] is followed, which requires manual configuration.

3.2. RIPng

Specified in [RFC2080], but no document specifying how it would be used in a Homenet environment has been written.

1. Reachability. YES, RIPng can detect reachability.

2. Border detection. NO. Any node which the router uses as a next hop, but which is not speaking RIPng, may be assumed to be an external border. However, the router will have to be manually configured, or use another routing protocol, to establish a path to that next hop; therefore auto-configured RIPng by itself does

not detect borders.

A. Any border. NO. Some ISPs use RIP (though rarely RIPng) to communicate with customers.

B. Find "up". NO. Manual configuration of the router neighboring the ISP is required to set a default route.

C. Border method. MANUAL.

3. Handles change. YES. RIPng normally handles router additions and removals. It may not be able to handle being moved from one existing segment to another.

4. No config. YES.

5. (null)

6. Multiple upstreams. NO, RIPng does not forward to multiple paths for the same prefix.

   A. Split up views. YES, RIPng can carry multiple paths, including specific routes for a wireles home agent, video cluster, or VPN concentrator. It cannot, by itself, establish routing policies determining which hosts may use those paths, so the upstream ISP may not have a return path (or may have an asymmetric path).

   B. (null)

   C. Multiple PD. Yes, RIPng can support multiple prefixes on a link.

   D. (null)

   E. Failover. Yes, RIPng can calculate a new path when one is lost or withdrawn.

   F. Walled garden. SOMEWHAT. RIPng can carry destination routes, but cannot by itself support source-based routing.

   G. (null)

7. Non-hierarchical addressing. YES.

8. Failover. YES.

9. Prevent loops. SOMEWHAT. RIPng uses the original RIP count-to-infinity algorithm to prevent infinite loops; it works, but is inefficient, especially in larger networks.

10. Lightweight. YES.

11. Robust to MDUs. YES.

12. Wireless. YES.

13. Unintended joins. NO. There is no authorization method; [RFC2080] says to use the Authentication Header built into IPv6, which would allow any RIPng host.

3.3. UP-PIO

As documented in [UP-PIO], this proposal would overload Router Advertisements to apporximate a distance-vector routing protocol.

1. Reachability. YES, UP-PIO will find a path, but it may not be the shortest path.

2. Border detection. YES. UP-PIO infers from DHCP-PD where the ISP network is.

   A. Any border. YES. A dedicated gateway, intended to run between an 802.15.4 network and a Wi-Fi or Ethernet (etc.) segment on a Homenet network, could be preconfigured to establish itself as UP for that prefix.

   B. Find "up". YES.

   C. Border method. Assume that DHCP-PD indicates upstream ISP, increment distance with RAs.

3. Handles change. YES, UP handles moves/adds/changes/deletions exactly as well as Router Advertisements do.

4. No config. YES.

5. (null)

6. Multiple upstreams. YES, whatever information is included in RAs is propagated.

   A. Split up views. YES.

B. (null)

C. Multiple PD. YES.

D. (null)

E. Failover.

F. Walled garden. YES.

G. (null)

7. Non-hierarchical addressing. NO. UP depends on hierarchical addressing.

8. Failover. YES, when RAs are no longer detected, an alternate path is computed.

9. Prevent loops. Undefined; the protocol is still being defined. It is expected to prevent loops as well as RIPng.

10. Lightweight. YES.

11. Robust to MDUs. YES.

12. Wireless. YES.

13. Unintended joins. NO. Even SEND would only authenticate, not authorize.

3.4. IS-IS

As defined in [RFC1195], but no document specifying how it would be used in a Homenet environment has been written.

1. Reachability. YES.

2. Border detection. NO. Any node which the router uses as a next hop, but which is not speaking IS-IS, may be assumed to be an external border. However, the router will have to be manually configured, or use another routing protocol, to establish a path to that next hop; therefore auto-configured IS-IS by itself does not detect borders.

A. Any border. NO.

B. Find "up". NO. Manual configuration of the router neighboring the ISP is required to set a default route.

C. Border method. MANUAL.

3. Handles change. YES.

4. No config. NO, IS-IS must be configured.

5. (null)

6. Multiple upstreams. YES.

   A. Split up views. YES.

   B. (null)

   C. Multiple PD. YES.

   D. (null)

   E. Failover. YES.

   F. Walled garden. YES.

   G. (null)

7. Non-hierarchical addressing. YES.

8. Failover. YES.

9. Prevent loops. YES.

10. Lightweight. NO.

11. Robust to MDUs. YES.

12. Wireless. YES.

13. Unintended joins. SOMEWHAT, if [RFC5310] is implemented, but that requires further manual configuration.

3.5. MANEMO

No document exists describing this mechanism, though several people have suggested it to the working group. Evaluation will have to be undertaken by someone familiar with the mechanism.

1. Reachability

2. Border detection

   A. Any border.

   B. Find "up".

   C. Border method.

3. Handles change.

4. No config

5. (null)

6. Multiple upstreams.

   A. Split up views.

   B. (null)

   C. Multiple PD.

   D. (null)

   E. Failover.

   F. Walled garden.

   G. (null)

7. Non-hierarchical addressing.

8. Failover.

9. Prevent loops.

10. Lightweight.

11. Robust to MDUs.

12. Wireless.

13. Unintended joins.

3.6. RPL

As documented in [RPL], but no document specifying how it would be used in a Homenet environment has been written.

1. Reachability. YES.

2. Border detection. NO.

    A. Any border. NO.

    B. Find "up". NO.

    C. Border method. NO.

3. Handles change. YES.

4. No config. YES?

5. (null)

6. Multiple upstreams.

    A. Split up views.

    B. (null)

    C. Multiple PD.

    D. (null)

    E. Failover.

    F. Walled garden.

    G. (null)

7. Non-hierarchical addressing.

8. Failover.

9. Prevent loops.

10. Lightweight. YES.

11. Robust to MDUs.

12. Wireless.

13. Unintended joins.

3.7. new section

Requirement	OSPFv3	RIPng	UP PIO	IS-IS	MANEMO	RPL
1.	YES	YES	YES	YES		
2.	NO	NO	YES	NO		
2A.	NO	NO	YES	NO		
2B.	NO	NO	YES	NO		
2C.	MANUAL	MANUAL	PD	MANUAL		
3.	YES	YES	YES	YES		
4.	YES	YES	YES	NO		
5.	NA	NA	NA	NA		
6.	YES	NO	YES	YES		
6A.	SOME	YES	YES	YES		
6B.	NA	NA	NA	NA		
6C.	YES	YES	YES	YES		
6D.	NA	NA	NA	NA		
6E.	YES	YES	YES	YES		
6F.	SOME	SOME	YES	YES		
6G.	NA	NA	NA	NA		
7.	YES	YES	NO	YES		
8.	YES	YES	YES	YES		
9.	YES	SOME	TBD	YES		
10.	NO	YES	YES	NO		
11.	YES	YES	YES	YES		
12.	YES	YES	YES	YES		
13.	NO	NO	NO	SOME		

4. Security Considerations

As an evaluation document, no security considerations are created. The solution should be safe from route injection to perpetrate man-in-the-middle attacks, especially in multi-dwelling or other dense/ mesh networks, but this may be a link requirement more than a routing requirement.

5. IANA Considerations

There are no IANA considerations or implications that arise from this document.

6. Informative References

[OSPFV3-AUTH-TRAILER]
"".

[OSPFv3-autoconfig]
"draft-acee-ospf-ospfv3-autoconfig".

[RFC1195] "Use of OSI IS-IS for Routing in TCP/IP and Dual Environments".

[RFC2080] R. Minnear, "RIPng for IPv6".

[RFC5310] "IS-IS Generic Cryptographic Authentication".

[RPL] "draft-ietf-roll-rpl-19".

[UP-PIO] "draft-howard-up-pio-00".

[draft-howard-homenet-routing-requirements]
"Homenet Routing Requirements", December 2011.

[draft-ietf-homenet-arch]
"Home Networking Architecture for IPv6".

Author's Address

Lee Howard
Time Warner Cable
13820 Sunrise Valley Drive
Herndon, VA 20171
US

Phone: +1 703 345 3513
Email: lee.howard@twcable.com