

Routing Protocol Selection

Homenet WG

IETF 91, Hawaii

Nov 11, 2014

From IETF 89:

“Zero, One or 2+ Routing Protocols”

1. “Zero Routing Protocol” implies
 - “HNCP Fallback” using configuration topology
 - Will manage to get packets out the uplink that corresponds to the DHCPv6 PD prefix
 - No metrics, not necessarily shortest path, etc.

2. “One Routing Protocol” implies
 - Do not use “HNCP Fallback”
 - Choose one of OSPF, IS-IS, Babel, etc.

If we decide to do #2 and fail, we probably end up with #3

STRONG HUM ↑

WEAK HUM ↓

3. “2 or more protocols” implies
 - No decision on which routing protocol to use in the home
 - Some way to ensure that the routing protocol used is supported by all routers in a given homenet (HNCP has a rudimentary mechanism for this)
 - HNCP Fallback in case no common routing protocol is found

From IETF 90:

Ideas for the process of selecting a routing protocol

1. Compare existing protocols
 - Set a date
 - Define what it means to be an “existing protocol”
 - Identify “existing protocols” on that date
 - RFC 5218 as a guide to select one
2. Write a requirements document
 - Risk of becoming a discussion about traits of existing protocols rather than requirements we need
3. Coin Flip
4. Something else?

Please Discuss.
We have until 9:25am
We don't have to come up with a decision today.

Today:

Ideas for the process of selecting a routing protocol

1. Compare existing protocols
 - Set a date
 - Define what it means to be an “existing protocol”
 - Identify “existing protocols” on that date
 - RFC 5218 as a guide to select one
2. Write a requirements document
 - Risk of becoming a discussion about traits of existing protocols rather than requirements we need
3. Coin Flip
4. Something else?

IETF 90 Minutes:

<http://tinyurl.com/hnet90>

Please Discuss Again.

We have until 10:00 am

It would be nice to come up with a decision this time.

RFC 5218: Potential Success Factors

1. Positive net value (meet a real need)
2. Incremental deployability
3. Open code availability
4. Freedom from usage restrictions
5. Open spec availability
6. Open development and maintenance processes
7. Good technical design (see RFC 1958)

Additional “wild” success factors:

8. Threats sufficiently mitigated
9. Extensible
10. No hard scalability bound