Architecture Discussion – Conclusions

Homenet Interim,
October 2011

Jari Arkko
Tim Chown

Update from discussions

Has been useful for feedback on the architecture principles

Some interesting discussions, e.g.

- Homenet “versions”
- Security borders
- Prefix configuration methods
- Routing mechanisms

Some Key Conclusions & Non-Conclusions

Key Conclusions (1/3)

Focus on running code + some improvements

We could do “baseline” version 1 home and then add improvements later

Route where you had an IPv4 NAT seems acceptable

Running IPv6-only networks requires us to document additional considerations

We understand the requirements for prefix assignment within the home network

Key Conclusions (2/3)

Link state routing protocol (OSPF etc) seems potentially doable & could solve prefix assignment and other problems relatively easily

LLNs, virtual machines, etc. can attach to home networks and either participate in the same manner or map to their internal mechanisms

If there is multihoming support, it is primarily about using the right source address to avoid ingress filtering, the rest is up to the hosts and applications

Key Conclusions (3/3)

Not happy with Simple Security

Need to discover borders

Need to do discovery and naming across subnets

Key Non-Conclusions

Still some disagreement on whether we need to support arbitrary topologies

Is multihoming part of version 1?

What, if anything, we should do instead of Simple Security

If we need a way to indicate source of traffic (local/Internet), is ULA the right way to do it?

Discovery mechanisms (proxy vs. extend)

Relationship of multicast and unicast DNS systems

Possible Homenet Recommendations, Take 2

- Use an IPv6 router where you have an IPv4 NAT
- Use multiple subnets
- External prefix delegation from the ISP
- Internal stable & efficient prefix assignment
- Use OSPF with prefix assignment extensions
- Local DNS servers & cross-subnet mcast DNS
- Implement Simple Security + PCP + extensions

Other Conclusions

On re-use of existing protocols

Desirable to reuse existing protocols

Conservative approach

- Give some weight to running code
- But new capabilities are required
- Need to know new protocols will be implemented
  - Some depends on open source development

Backwards compatibility

- But don’t be concerned about existing broken deployments (e.g. /64 due to CPE limitations)

On Topology Assumptions

No built-in assumptions

- Make the least assumptions possible

Users want simple plug and play of devices

- But what about arbitrary topologies/loops?
- Enough to say do not introduce new IPv6 cases that would break with IPv4+NAT?

Do we include multi-homing?

- Is 2nd ISP for resilience unrealistic to consider?
- Is work valid without multi-homed scenario?

On dual-stack

Assume one of two cases
- Dual-stack IPv4-IPv6, or IPv6 only

IPv6 solutions must not adversely affect IPv4

Seek to keep IPv4 and IPv6 topologies congruent where possible
- But with largest possible subnets

Specific transition tools out of scope
- Though IPv6-only homenet may need to reach external IPv4 content

Largest possible subnets

IPv4 home network deployments are most commonly single subnet

- Initial IPv6 deployments probably the same

Seek to use largest possible subnets

- Route in IPv6 where IPv4 NAT is used

There are chained IPv4 NATs out there

- e.g. VMs like Parallels, ICS, etc
- Will we need IPv6 routed versions of these?

Transparent end-to-end

IPv6 architecture allows transparent end-to-end
- In practice depends on firewall mode (RFC 6092)
- Or whether we use “Advanced Security”

RFC 6092 default is to block
- But all IPv6 nodes should still be globally addressable even if not globally reachable
- RFC 6092 requires support for “transparent” mode

Need traversal tools if firewalls are default deny
- Implies PCP or uPnP signaling through multiple routers

Routing functionality

Desirable that routers have knowledge of the topology

- Implies use of OSPF or IS-IS
- Coordinate LSA and RA usage?

Zeroconf OSPF (zospf) may be attractive

- Could provide prefix configuration
- Across single area with shared pw, defines boundaries

Supporting multi-homing adds complexity

- May imply need support for source routing in some form

Different protocols for different media properties

- RPL within low power/lossy networks

Self-organising network

Should be self-organising and self-configuring

- Minimal configuration, e.g. WLAN pw, router pw

Need “automatic border detection”

- And know where to apply security
- Relevant for site scope border for multicast

Stable prefixes “under normal conditions”

- But re-plumbing may cause prefix changes

No requirement to aggregate internally?

- Although hierarchical prefix configuration may avoid need to use dynamic routing protocol?

Naming and Discovery

Naming and service discovery should work across the whole homenet
But may wish to have policy borders

- e.g. for guest network

Existing protocols link-layer constrained

- We seem to prefer extending discovery scope rather than discovery protocol proxies

Need naming system that can be used internally or externally

- Consider domain labels

- Consider services not just devices

Adapt to ISP constraints

Assume at least a /60, preferably a /56
Affects prefix configuration discussion

Should assume static prefixes
Privacy implications of that out of scope

Homenet prefix from ISP *may* change
So don’t make renumbering harder than need be

Also, internal reorganisation may lead to renumbering of some links

The “walled garden” rathole

Hot Discussion Topics from the Days

- Approaches to standardizing homenets
- Topology
- Multihoming
- Prefix distribution requirements and mechanisms
- Routing solutions
- Advanced security