Network Working Group	J. Arkko
Internet-Draft	Ericsson
Intended status: Informational	M. Townsley
Expires: January 06, 2012	Cisco
	July 05, 2011

Home Networking Architecture for IPv6
draft-arkko-townsley-homenet-arch-00

Abstract

This memo focuses on the evolving networking technology within and among relatively small "residential home" networks. The goal of this memo is to define the architecture for IPv6-based home networking that supports the demands placed on it. This architecture shows how standard IPv6 mechanisms and addressing can be employed in home networking, and outlines the need for specific protocol extensions for certain additional functionality.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This memo focuses on the evolving networking technology within and among relatively small "residential home" networks and the associated challenges. For example, an obvious trend in home networking is the proliferation of networking technology in an increasingly broad range and number of devices. This evolution in scale and diversity sets some requirements on IETF protocols. Some of these requirements relate to the need for supporting multiple subnets for private and guest networks, the introduction of IPv6, and the introduction of specialized networks for home automation and sensors.
While many advanced home networks have been built, most operate based on IPv4, employ solutions that we would like to avoid such as network address translation (NAT), or require an expert assistance to set up. The architectural constructs in this document are focused on the problems to be solved when introducing IPv6 with a eye towards a better result than what we have today with IPv4, as well as a better result than if the IETF had not given this specific guidance.
This architecture document aims to provide the basis for how standard IPv6 mechanisms and addressing [RFC2460] [RFC4291] can be employed in home networking, while coexisting with existing IPv4 mechanisms that are widely deployed.

2. Effects of IPv6 on Home Networking

Service providers are deploying IPv6, widely accessed content is becoming available on IPv6, and support for IPv6 is increasingly available in devices and software used in the home. While IPv6 resembles IPv4 in many ways, it changes address allocation principles and allows direct IP addressability and routing to devices in the home

from the Internet. Following is an overview of some of the areas of that are both promising and problematic:

Multiple segments

While less complex L3-topologies involving as few subnets as possible are preferred in home networks for a variety of reasons including simpler management and service discovery, incorporation of dedicated segments remain necessary for some cases. For instance, a common feature in modern home routers in the ability to support both guest and private network segments. Also, link layer networking technology is poised to become more heterogeneous, as networks begin to employ both traditional Ethernet technology and link layers designed for low-powered sensor networks. Finally, similar needs for segmentation may occur in other cases, such as separating building control or corporate extensions from the Internet access network. Different segments may be associated with subnets that have different routing and security policies.

Documents that provide some more specific background and depth on this topic include: [I-D.herbst-v6ops-cpeenhancements], r *[I-D.baker-fun-multi-router]*, and [I-D.baker-fun-routing-class].

In addition to routing, rather than natting, between subnets, there are issues of when and how to extend mechanisms such as service discovery which currently rely on link-local addressing to limit scope.

Security, Borders, and the elimination of NAT

The End-to-end communication that is promised with IPv6 is both an incredible opportunity for innovation and easy of network operation, but it is also a concern as it it exposes nodes in the internal networks to receipt of otherwise unwanted traffic from the Internet. Firewalls that restrict incoming connections may be used to prevent exposure, however, this reduces the efficacy of end-to-end connectivity that IPv6 has the potential to restore. [RFC6092] provides recommendations for an IPv6 firewall that applies "limitations on end-to-end transparency where security considerations are deemed important to promote local and Internet security." The firewall operation is "Simple" in that there is an assumption that traffic which is to be blocked by default is defined in the RFC and not expected to be updated by the user or otherwise. Advanced Security for IPv6 CPE *[I-D.vyncke-advanced-ipv6-security]* takes the approach that in order to provide the greatest end-to-end transparency as well as security, security polices must be updated by a trusted party which can provide intrusion signatures an other "active" information on security threats. This is much like a virus-scanning tool which must receive updates in order to detect and/or neutralize the latest attacks as they arrive. As the name implies

"Advanced" security requires significantly more resources and infrastructure (including a source for attack signatures) vs. "Simple" security.

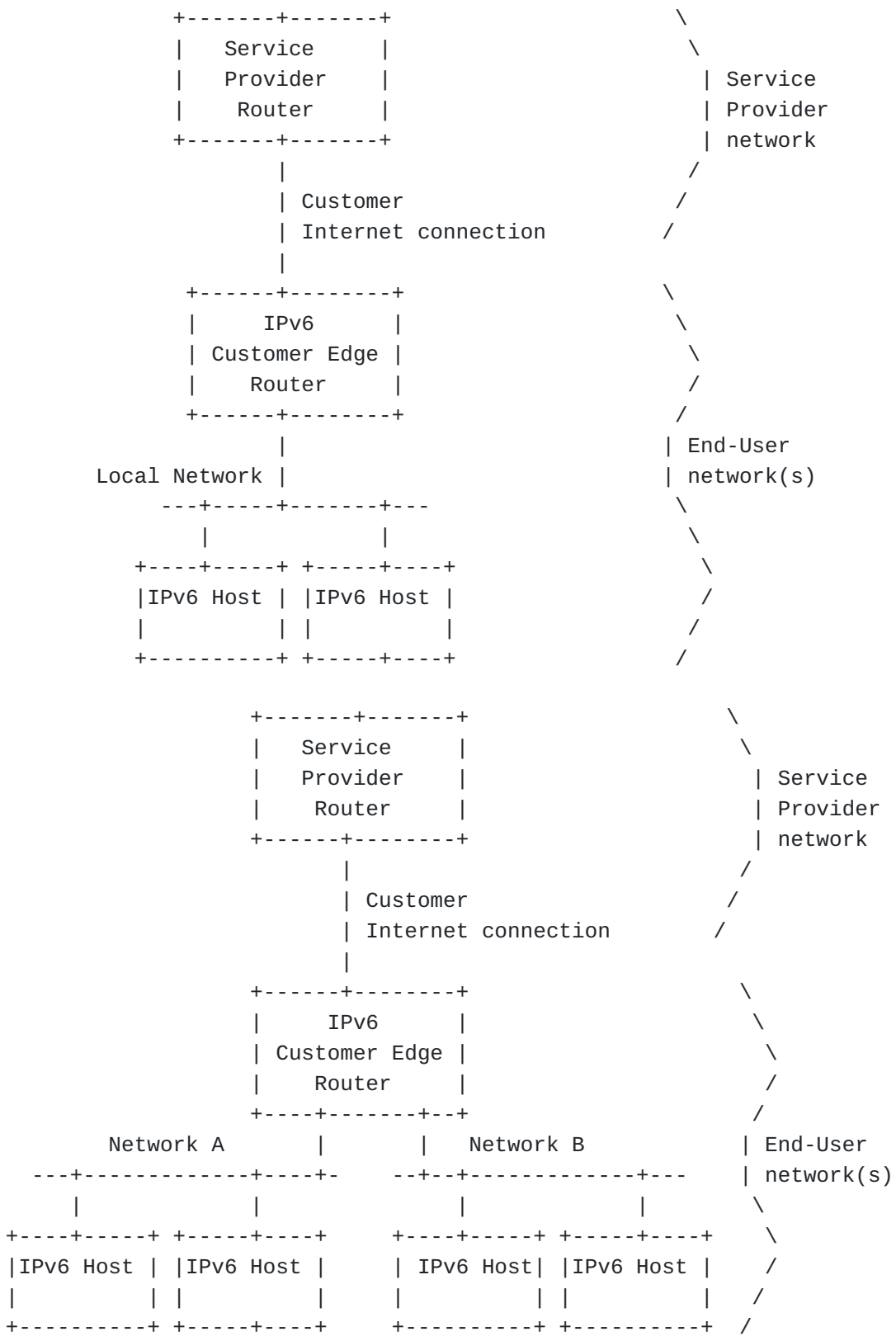
In addition to the security mechanisms themselves, it is important to know where to enable them. If there is some indication as to which router is connected to the "outside" of the home network, this is feasible. Otherwise, it can be difficult to know which security policies to apply where. Further, security policies may be different for various address ranges if ULA addressing is setup to only operate within the homenet itself and not be routed to the Internet at large.

Naming, and manual configuration of IP addresses

In IPv4, it is common practice to reach a router for configuration, DNS resolver functions, or otherwise via 192.168.1.1 or some other well-known RFC 1918 address. In IPv6, there is no such address space available, and generally IPv6 addresses are more cumbersome for humans to manually configure. As such, even for the simplest of functions, naming and the associated discovery of service is imperative for an easy to administer homenet.

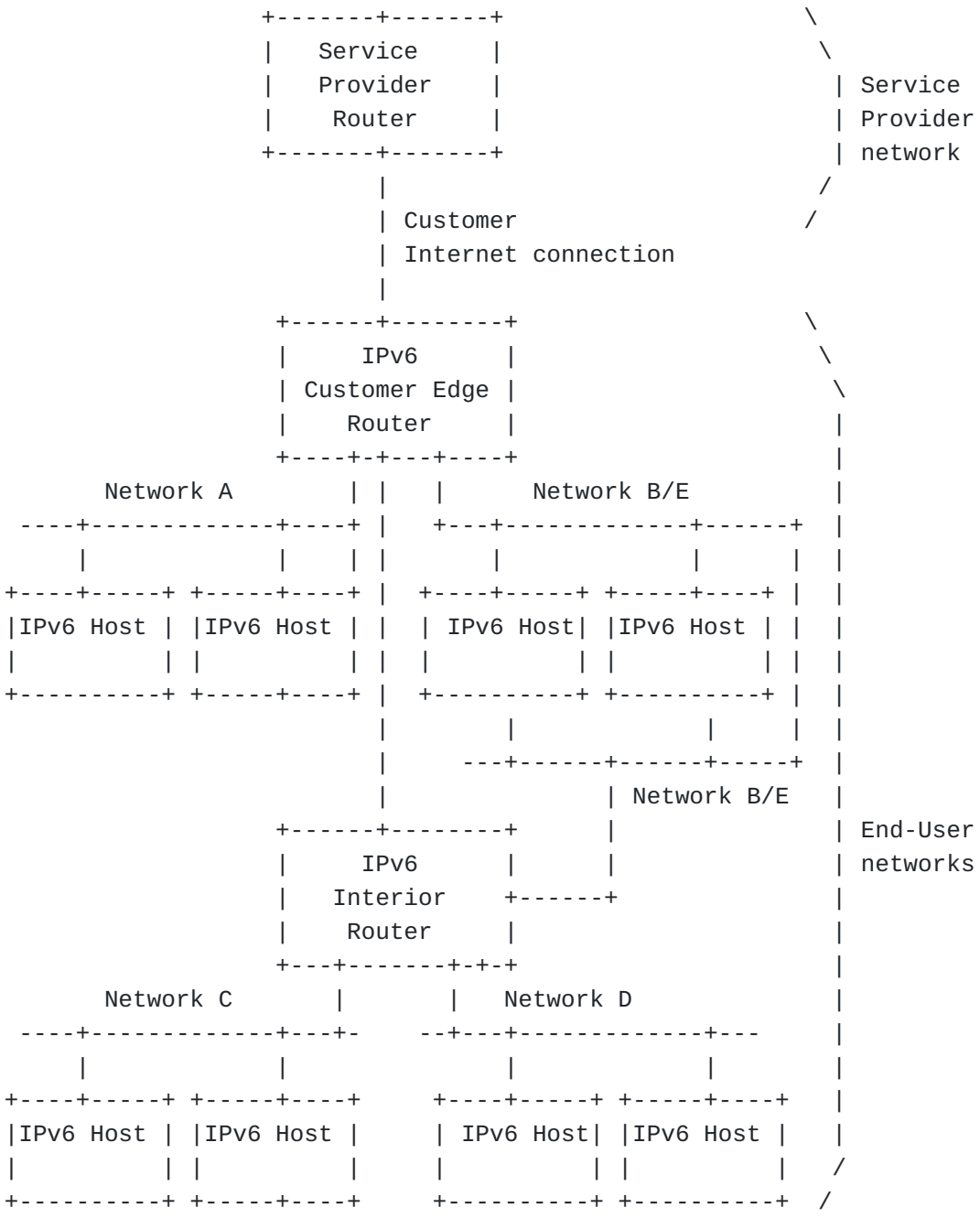
3. Architecture

An architecture outlines how to construct home networks involving multiple routers and subnets. In the following this memo presents a few typical home network topology models, followed by architectural principles that govern how the various nodes should work together. Finally, some guidelines are given for realizing the architecture with the IPv6 addressing architecture, prefix delegation, global and ULA addresses, source address selection rules and other existing components of the IPv6 architecture. The architecture also drives what protocols extensions are necessary, as will be discussed in Section 3.3.



...
Figure 3 shows a little bit more complex network with two routers and eight devices connected to one ISP. This network is similar to the one discussed in [I-D.ietf-v6ops-ipv6-cpe-router-bis]. The main

complication in this topology compared to the ones described earlier is that there is no longer a single router that a priori understand the entire topology. The topology itself may also be complex, it may not be possible to assume a pure tree form, for instance.



3.1. Requirements

[RFC6204] defines "Basic" requirements for IPv6 Customer Edge Routers, while [I-D.ietf-v6ops-ipv6-cpe-router-bis] describes "advanced" features. In general, home network equipment needs to cope with different types of network topologies discussed above. Manual

configuration is rarely, if at all, possible. The equipment needs to be prepared to handle at least

*prefix configuration for routers

*managing routing

*name resolution

*service discovery

*network security

Additional requirements may stem from support for multi-homing or multiple exit routers [I-D.baker-fun-multi-router].

3.2. Principles

There is little that the Internet standards community can do about the physical topologies or the need for some networks to be separated at the network layer for policy or link layer compatibility reasons. However, there is a lot of flexibility in using IP addressing and internetworking mechanisms. It would be desirable to provide some guidance on how this flexibility should be used to provide the best user experience and ensure that the network can evolve with new applications in the future.
The authors believe that the following principles guide us in designing these networks in the correct manner:

3.3. Implementing the Architecture on IPv6

The necessary mechanisms are largely already part of the IPv6 protocol set and common implementations. The few known counter-examples are discussed in the following. For prefix configuration, existing protocols are likely sufficient, but may at worst may need some small enhancements, such as new options. For automatic routing, it is expected that existing routing protocols can be used as is, however, a new mechanism may be needed in order to turn a selected protocol on by default. Support for multiple exit routers and multi-homing would also require extensions. For name resolution and service discovery, extensions to existing multicast-based name resolution protocols are needed to enable them to work across subnets.
The hardest problems in developing solutions for home networking IPv6 architectures include discovering the right borders where the domain "home" ends and the service provider domain begins, deciding whether some of necessary discovery mechanism extensions should affect only the network infrastructure or also hosts, and the ability to turn on routing, prefix delegation and other functions in a backwards compatible manner.

4. References

4.1. Normative References

[RFC2460]	Deering, S.E. and R.M. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.
[RFC4291]	Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, February 2006.
[RFC6092]	Woodyatt, J., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", RFC 6092, January 2011.
[RFC6204]	Singh, H., Beebee, W., Donley, C., Stark, B. and O. Troan, "Basic Requirements for IPv6 Customer Edge Routers", RFC 6204, April 2011.

4.2. Informative References

[I-D.baker-fun-multi-router]	Baker, F, "Exploring the multi-router SOHO network", Internet-Draft draft-baker-fun-multi-router-00, July 2011.
[I-D.baker-fun-routing-class]	Baker, F, "Routing a Traffic Class", Internet-Draft draft-baker-fun-routing-class-00, July 2011.
[I-D.herbst-v6ops-cpeenhancements]	Herbst, T and D Sturek, "CPE Considerations in IPv6 Deployments", Internet-Draft draft-herbst-v6ops-cpeenhancements-00, October 2010.
[I-D.vyncke-advanced-ipv6-security]	Vyncke, E, Yourtchenko, A and M Townsley, "Advanced Security for IPv6 CPE", Internet-Draft draft-vyncke-advanced-ipv6-security-03, October 2011.
[I-D.ietf-v6ops-ipv6-cpe-router-bis]	Singh, H, Beebee, W, Donley, C, Stark, B and O Troan, "Advanced Requirements for IPv6 Customer Edge Routers", Internet-Draft draft-ietf-v6ops-ipv6-cpe-router-bis-01, July 2011.

Appendix A. Acknowledgments

The authors would like to thank to Stuart Cheshire, James Woodyatt, Ole Troan, Lars Eggert, Ray Bellis, David Harrington, Wassim Haddad, Heather Kirksey, Dave Thaler, Fred Baker, and Ralph Droms for interesting discussions in this problem space.

Authors' Addresses

Jari Arkko Arkko Ericsson Jorvas, 02420 Finland EMail: jari.arkko@piuha.net

Mark Townsley Townsley Cisco Paris, 75006 France EMail: townsley@cisco.com