

Network Working Group
Internet-Draft
Intended status: Informational
Expires: January 13, 2014

C. Grundemann
C. Donley
CableLabs
J. Brzozowski
Comcast Cable Communications
L. Howard
Time Warner Cable
V. Kuarsingh
Rogers Communications
July 12, 2013

A Near Term Solution for Home IP Networking (HIPnet)
draft-grundemann-hipnet-00

Abstract

Home networks are becoming more complex. With the launch of new services such as home security, IP video, Smart Grid, etc., many Service Providers are placing additional IPv4/IPv6 routers on the subscriber network. This document describes a self-configuring home router that is capable of operating in such an environment, and that requires no user interaction to configure it. Compliant with [draft-ietf-homenet-arch](#), it uses existing protocols in new ways without the need for a routing protocol.

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 [RFC 2119](#) [[RFC2119](#)].

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <http://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on January 13, 2014.

Internet-Draft

[draft-grundemann-hipnet](#)

July 2013

Copyright Notice

Copyright (c) 2013 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1.	Introduction	3
1.1.	Requirements Language	3
2.	Terminology	3
3.	Architecture	4
3.1.	Current End-User Network Architecture	5
3.2.	HIPNet End-User Network Architecture	5
4.	Network Detection	6
4.1.	Edge Detection	6
4.2.	Directionless Home Routers	7
5.	Routing and Addressing	9
5.1.	Recursive Prefix Delegation	9
5.2.	Prefix Sub-Delegation Requirements	11
5.3.	Multiple Address Family Support	11
5.4.	Hierarchical Routing	12
6.	Multiple ISPs	12
6.1.	Backup Connection	12
6.2.	Multi-homing	13
6.2.1.	Multihoming Requirements	15
7.	Multicast Support	15
7.1.	Service Discovery	15
7.2.	Multicast Proxy Support	15
7.3.	Multicast Requirements	15
8.	Firewall Support	16
8.1.	Requirements	17
9.	Running Code	18
10.	IANA Considerations	18

11.	Security Considerations	18
12.	Acknowledgements	18
13.	References	18
13.1.	Normative References	18
13.2.	Informative References	19

Authors' Addresses	20
------------------------------	--------------------

[1.](#) Introduction

This document expands upon [[I-D.ietf-v6ops-6204bis](#)] to describe IPv6/IPv4 features for a residential or small-office router, referred to as a HIPnet router. Consistent with [[I-D.ietf-homenet-arch](#)], it focuses on network technology evolution to support increasingly large residential/SoHo networks. While the primary focus is on IPv6 support, this document also describes how to leverage IPv6 to configure IPv4 in a manner better than nested NATs in operation on many networks today.

This document specifies how a HIPnet router automatically detects both the edge of the customer network and its upstream interface, how it subdivides an IPv6 prefix to distribute to downstream routers, and how it leverages IPv6 address assignment to distribute IPv4 addresses. It also discusses how such a router can operate with a backup ISP or limited multihoming across two ISPs.

This document is an update to and replacement of [[I-D.grundemann-homenet-hipnet](#)].

[1.1.](#) 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 [RFC 2119](#) [[RFC2119](#)].

[2.](#) Terminology

End-User Network one or more links attached to the HIPnet router that connect IPv6 and IPv4 hosts.

Home IP Network (HIPnet) Router a node intended for home or small-office use that forwards packets not

explicitly addressed to itself.

Customer Edge Router (CER) a HIPnet router that connects the end-user network to a service provider network.

Internal Router an additional HIPnet router deployed in the home or small-office network that is not attached to a service provider network. Note that this is a functional role; it is expected that there will not be a difference in hardware or software between a CER and IR, except in such cases when a

Grundemann, et al.

Expires January 13, 2014

[Page 3]

Internet-Draft

[draft-grundemann-hipnet](#)

July 2013

CER has a dedicated non-Ethernet WAN interface (e.g. DSL/cable/ LTE modem) that would preclude it from operating as an IR.

Down Interface a HIPnet router's attachment to a link in the end-user network on which it distributes addresses and/or prefixes. Examples are Ethernet (simple or bridged), 802.11 wireless, or other LAN technologies. A HIPnet router may have one or more network-layer down interfaces.

downstream router a router directly connected to a HIPnet router's Down Interface.

Service Provider an entity that provides access to the Internet. In this document, a service provider specifically offers Internet access using IPv6, and may also offer IPv4 Internet access. The service provider can provide such access over a variety of different transport methods such as DSL, cable, wireless, and others.

Up Interface a HIPnet router's attachment to a link where it receives one or more IP addresses and/or prefixes. This is also the link to which the HIPnet router points its default route.

depth	the number of layers of routers in a network. A single router network would have a depth of 1, while a router behind a router behind a router would have a depth of 3.
width	The number of routers that can be directly subtended to an upstream router. A network with three directly attached routers behind the CER would have a width of 3.

[3.](#) Architecture

Grundemann, et al. Expires January 13, 2014 [Page 4]

Internet-Draft [draft-grundemann-hipnet](#) July 2013

[3.1.](#) Current End-User Network Architecture

An end-user network will likely support both IPv4 and IPv6. A typical end-user network consists of a "plug and play" router with IPv4 NAT functionality and a single link behind it, connected to the service provider network.

A typical IPv4 NAT deployment by default blocks all incoming connections. Opening of ports is typically allowed using a Universal Plug and Play Internet Gateway Device (UPnP IGD) [UPnP-IGD] or some other firewall control protocol.

Rewriting addresses on the edge of the network allows for some rudimentary multihoming, even though using NATs for multihoming does not preserve connections during a fail-over event [[RFC4864](#)].

Many existing routers support dynamic routing, and advanced end-users can build arbitrary, complex networks using manual configuration of address prefixes combined with a dynamic routing protocol.

[3.2.](#) HIPNet End-User Network Architecture

The end-user network architecture should provide equivalent or better capabilities and functionality than the current architecture. However, as end-user networks become more complex, the HIPnet architecture needs to support more complicated networks. Figure 1 illustrates the model topology for the end-user network.

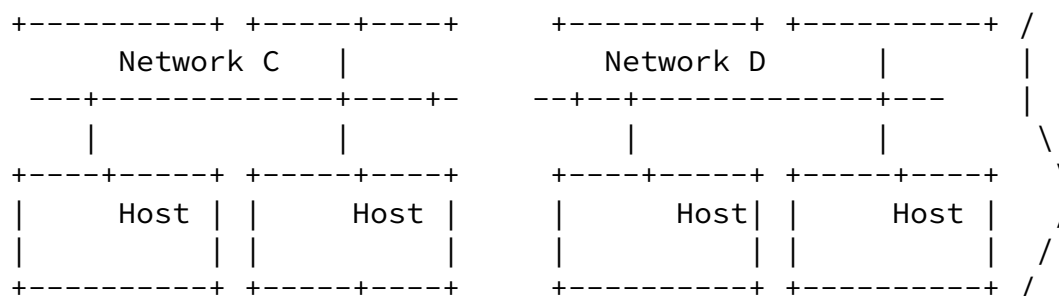
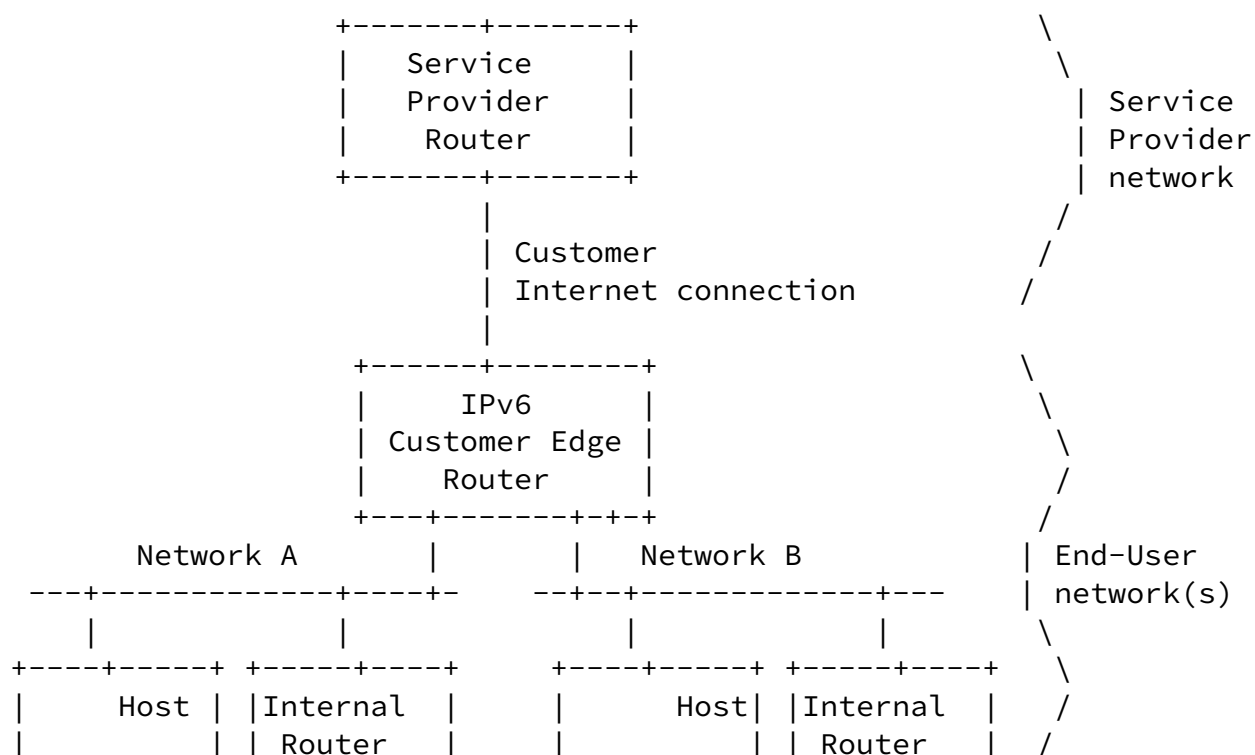


Figure 1: Example End-User Network

This architecture describes the following:

- o Prefix subdelegation supporting multiple subnets and routers

- o Border Detection
- o Router directionality supporting a hierarchical network
- o Multicast forwarding rules to support common service discovery protocols

While routers described in this document may be manually configured in an arbitrary topology with or without a dynamic routing protocol, this document only addresses automatic provisioning and configuration.

[4.](#) Network Detection

In multirouter home networks, routers have to determine where they fit in the topology – whether they are at the edge or internal, and which interface is up (that is, which interface points out of the network).

[4.1.](#) Edge Detection

Customer Edge Routers (CER) will often be required to behave differently from Internal Routers (IR) in several capacities. Some examples include: Firewall settings, IPv4 NAT, ULA generation (if supported), name services, multicast forwarding differences, and others. This is a functional role, and will not typically be differentiated by hardware/software (i.e. end users will not purchase a specific CER model of router distinct from IR models).

There are three methods that a router can use to determine if it is a CER for its given network:

"/48 Check" Service providers will provide IPv6 WAN addresses (DHCPv6 IA_NA) and IPv6 prefixes (DHCPv6 IA_PD) from different pools of addresses. The largest IPv6 prefix that we can expect to be delegated to a home router is a /48. Combining these two observations, a home router can compare the WAN address assigned to it with the prefix delegated to it to determine if it is attached directly to a service provider network. If the router is a CER, the WAN address will be from a different /48 than the

prefix. If the router is an IR, the WAN address will be from the same /48 as the prefix. In this way, the router can determine if it is receiving an "external" prefix from a service provider or an "internal" prefix from another home router.

CER_ID A home router can use the CER_ID DHCPv6 option defined in [[I-D.donley-dhc-cer-id-option](#)] to determine if it is a CER or an IR. ISPs will not set the CER_ID option, but the first CPE router sets its address in the option and other routers forward the completed CER_ID to subdelegated routers.

Physical Some routers will have a physical differentiator built into them by design that will indicate that they are a CER. Examples include mobile routers, DSL routers, and cable eRouters. In the case of a mobile router, the presence of an active cellular connection indicates that the router is at the customer edge. Likewise, for an eRouter, the presence of an active DOCSIS(R) link tells the router that it is at the customer edge.

HIPnet routers can (and likely will) use more than one of the above techniques in combination to determine the edge. For example, an internal router will check for the CER_ID option, but will also use the 48 check in case its upstream router does not support CER_ID.

[4.2.](#) Directionless Home Routers

As home networks grow in complexity and scale, it will become more common for end users to make mistakes with the physical connections between multiple routers in their home or small office. This is likely to produce loops and improper uplink connections. While we can safely assume that home networks will become more complex over time, we cannot make the same assumption of the users of home networks. Therefore, home routers will need to mitigate these physical topology problems and create a working multi-router home network dynamically, without any end user intervention.

Legacy home routers with a physically differentiated uplink port are "directional;" they are pre-set to route from the 'LAN' or Internal ports to a single, pre-defined uplink port labeled "WAN" or "Internet". This means that an end-user can make a cabling mistake

which renders the router unusable (e.g. connecting two router's

uplink ports together). On the other hand, in enterprise and service provider networks, routers are "directionless;" that is to say they do not have a pre-defined 'uplink' port. While directional routers have a pre-set routing path, directionless routers are required to determine routing paths dynamically. Dynamic routing is often achieved through the implementation of a dynamic routing protocol, which all routers in a given network or network segment must support equally. This section introduces an alternative to dynamic routing protocols (such as OSPF) for creating routing paths on the fly in directionless home routers.

Note that some routers (e.g. those with a dedicated wireless/DSL/DOCSIS WAN interface) may continue to operate as directional routers. The HIPnet mechanism described below is intended for general-purpose routers.

The HIPnet mechanism uses address acquisition as described in [[I-D.ietf-v6ops-6204bis](#)] and various tiebreakers to determine directionality (up vs. down) and by so doing, creates a logical hierarchy (cf. [[I-D.chakrabarti-homenet-prefix-alloc](#)]) from any arbitrary physical topology:

1. After powering on, the HIPnet router sends Router Solicitations (RS) ([[RFC4861](#)]) on all interfaces (except Wi-Fi*)
2. Other routers respond with Router Advertisements (RA)
3. Router adds any interface on which it receives an RA to the candidate 'up' list
4. The router initiates DHCPv6 PD on all candidate 'up' interfaces. If no RAs are received, the router generates a /48 ULA prefix.
5. The router evaluates the offers received (in order of preference):
 - a) Valid GUA preferred (preferred/valid lifetimes >0)
 - b) Internal prefix preferred over external (for failover - see Section [6.1])
 - c) Largest prefix (e.g. /56 preferred to /60)
 - d) Link type/bandwidth (e.g. Ethernet vs. MoCA)
 - e) First response (wait 1 s after first response for additional offers)

f) Lowest numerical prefix

6. The router chooses the winning offer as its Up Interface.

Once directionality is established, the router continues to listen for RAs on all interfaces but doesn't acquire addresses on Down Interfaces. If the router initially receives only a ULA address on its Up Interface and GUA addressing becomes available on one of its Down Interfaces, it restarts the process. If the router stops receiving RAs on its Up Interface, it restarts the process.

In all cases, the router's Up Interface becomes its uplink interface; the router acts as a DHCP client on this interface. The router's remaining interfaces are Down Interfaces; it acts as a DHCP server on these interfaces. Also, per [[I-D.ietf-v6ops-6204bis](#)], the router only sends RAs on Down Interfaces.

*Note: By default, Wi-Fi interfaces are considered to point "down." This requires manual configuration to enable a wireless uplink, which is preferred to avoid accidental or unwanted linking with nearby wireless networks.

[5.](#) Routing and Addressing

HIPnet routers use DHCPv6 prefix sub-delegation ([[RFC3633](#)]) to recursively build a hierarchical network ([[I-D.chakrabarti-homenet-prefix-alloc](#)]). This approach requires no new protocols to be supported on any home routers.

Default router settings: Only CER instantiates guest network. Wifi defaults to 'down' direction, default route uses wired interface. Firewall considers Wifi an inside port. Wi-Fi bridged with first wired Down Interface.

[5.1.](#) Recursive Prefix Delegation

Once directionality is established, the home router will acquire a WAN IPv6 address and an IPv6 prefix per [[I-D.ietf-v6ops-6204bis](#)]. As HIPnet routers (other than the CER) do not know their specific location in the hierarchical network, all HIPnet routers use the same generic rules for recursive prefix delegation to facilitate route aggregation, multihoming, and IPv4 support (described below). This methodology expounds upon that previously described in [[I-D.chakrabarti-homenet-prefix-alloc](#)].

The process can be illustrated in the following way:

1. Per [[I-D.ietf-v6ops-6204bis](#)], the HIPnet router assigns a separate /64 from its delegated prefix(es) for each of its Down Interfaces in numerical order, starting from the numerically lowest.
2. If the received prefix is too small to number all Down Interfaces, the router collapses them into a single interface, assigns a single /64 to that interface, and logs an error message.
3. The HIPnet router subdivides the IPv6 prefix received via DHCPv6 ([[RFC3315](#)]) into sub-prefixes. To support a suggested depth of three routers, with as large a width as possible, it is recommended to divide the prefix on 2-, 3-, or 4-bit boundaries. If the received prefix is not large enough, it is broken into as many /64 sub-prefixes as possible and logs an error message. By default, this document suggests that the router divide the delegated prefix based on the aggregate prefix size and the HIPnet router's number of physical Down Interfaces. This is to allow for enough prefixes to support a downstream router on each down port.
 - * If the received prefix is smaller than a /56 (e.g. a /60),
 - + 8 or more port routers divide on 3-bit boundaries (e.g. /63).
 - + 7 or fewer port routers divide on 2-bit boundaries (e.g. /62).
 - * If the received prefix is a /56 or larger,
 - + 8 or more port routers divide on 4-bit boundaries (e.g. /60).
 - + 7 or fewer port routers divide on 3-bit boundaries (e.g. /59).
4. The HIPnet router delegates remaining prefixes to downstream

routers per [[RFC3633](#)] in reverse numerical order, starting with the numerically highest. This is to minimize the renumbering impact of enabling an inactive interface.

For example, a four port router with two LANs (two Down Interfaces) that receives 2001:db8:0:b0::/60 would start by numbering its two Down Interfaces with 2001:db8:0:b0::/64 and 2001:db8:0:b1::/64 respectively, and then begin prefix delegation by giving 2001:db8:0:bc::/62 to the first directly attached downstream router.

[5.2.](#) Prefix Sub-Delegation Requirements

PSD-1: The HIPnet router MUST support [[I-D.ietf-v6ops-6204bis](#)] address acquisition and LAN addressing.

PSD-2: The HIPnet router MUST support Delegating Router behavior for the IA-PD Option [[RFC3633](#)] on all Down Interfaces.

PSD-3: HIPnet routers MUST NOT act as both a DHCP client and server on the same link.

PSD-4: The HIPnet router MAY support other methods of dividing the received prefix.

PSD-5: The HIPnet router MUST delegate prefixes of the same size to downstream routers.

PSD-6: Per [[I-D.ietf-v6ops-6204bis](#)] L-2, the HIPnet router allocates a /64 to each Down Interface. The HIPnet router SHOULD allocate these /64 interface-prefixes in numerical order, starting with the lowest.

PSD-7: If there are insufficient /64s for each Down Interface, the HIPnet router SHOULD assign the lowest numbered /64 for all Down Interfaces and log an error message.

PSD-8: The HIPnet router MAY reserve additional /64 interface-prefixes for interfaces that will be enabled in the future.

PSD-9: The HIPnet router SHOULD delegate sub-prefixes to downstream routers starting from the numerically highest sub-prefix and working down in reverse numerical order.

PSD-10: If there are not enough sub-prefixes remaining to delegate to all downstream routers, the HIPnet router SHOULD log an error message.

[5.3.](#) Multiple Address Family Support

The recursive prefix delegation method described above can be extended to support additional address types such as IPv4, additional GUAs, or ULAs. When the HIPnet router receives its prefix via DHCPv6 ([\[RFC3633\]](#)), it computes its 8 or 16-bit Link ID (bits 56-64 or 48-64) from the received IA_PD. It then prepends additional prefixes received in one or more IPv6 Router Advertisements ([\[RFC4861\]](#)) or from the DHCPv4-assigned ([\[RFC2131\]](#)) IPv4 network address received on the Up Interface.

Grundemann, et al.

Expires January 13, 2014

[Page 11]

Internet-Draft

[draft-grundemann-hipnet](#)

July 2013

As the network is hierarchical, upstream routers know the Link ID for each downstream router, and know the prefix(es) on each LAN segment. Accordingly, HIPnet routers automatically calculate downstream routes to all downstream routers.

In networks using this mechanism for IPv4 provisioning, it is suggested that the CER use addresses in the 10.0.0.0/8 ([\[RFC1918\]](#)) range for downstream interface provisioning. When used with a 16-bit Link ID, this results in an IPv4 /24 created for each LAN segment (8 network bits plus 16 Link ID bits equals a 24 bit subnet mask).

[5.4.](#) Hierarchical Routing

The recursive prefix delegation method described above, coupled with "up detection", enables very simple hierarchical routing. By this we mean that each router installs a single default 'up' route and a more specific 'down' route for each prefix delegated to a downstream IR. Each of these 'down' routes simply points all packets destined to a given prefix to the WAN IP address of the router to which that prefix was delegated. This combination of a default 'up' route and more specific 'down' routes provides complete reachability within the home network with no need for any additional message exchange or routing protocol support.

[6.](#) Multiple ISPs

HIPnet routers can support either active/standby multihoming with multiple ISPs or limited active/active multihoming without a routing protocol.

6.1. Backup Connection

Using the procedure described above, multi-router home networks with multiple ISP connections can easily operate in an active/standby manner, switching from one Internet connection to the other when the active connection fails. Lacking a default priority, HIPnet routers will have to default to a "first online" method of primary CER selection. In other words, by default, the first CER to come online becomes the primary CER and the second CER to turn on becomes the backup. In this text, the primary ISP is the ISP connected to the primary CER and the backup ISP is simply the ISP attached to the backup CER.

In an active/standby multi-ISP scenario, a backup CER sets its Up Interface to point to the primary CER, not the backup ISP. Hence, it does not acquire or advertise the backup ISP prefix. Instead, it discovers the internally advertised GUA prefix being distributed by the currently active primary CER.

In the case of a primary ISP failure, per [[I-D.ietf-v6ops-6204bis](#)], the CER sends an RA advertising the preferred lifetime as 0 for the ISP-provided prefix, and its router lifetime as 0. The backup CER becomes active when it sees the primary ISP GUA prefix advertised with a preferred lifetime of 0. In the case of CER failure, if the backup CER sees the Primary CER stop sending RAs altogether, the Backup CER becomes active.

When the backup CER becomes active, it obtains and advertises its own external GUA. When advertising the GUA delegated by its ISP, the backup CER sets the valid, preferred, and router lifetimes to a value greater than 0. Other routers see this and re-determine the network topology via "up" detection, placing the new CER at the root of the new hierarchical tree.

Using this approach, manual intervention may be required to transition back to the primary ISP. This prevents flapping in the event of intermittent network failures. Another alternative is to

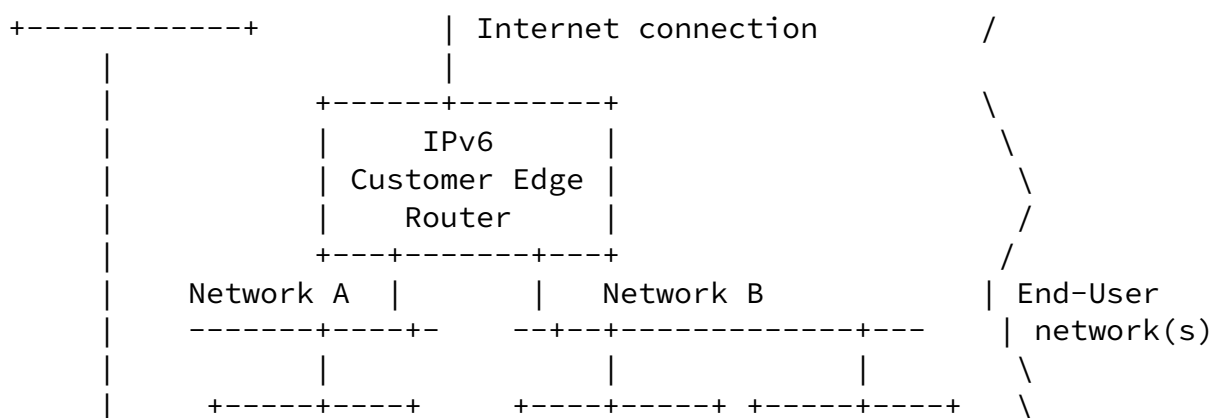
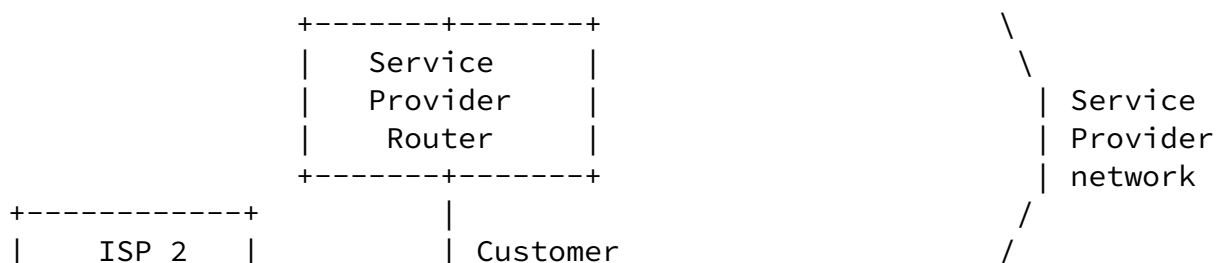
have a user-defined priority, which would facilitate pre-emption.

6.2. Multi-homing

The HIPnet algorithm also allows for limited active/active multihoming in two cases:

1. When one ISP router is used as the primary connection and the second ISP router is used for limited connectivity e.g. for a home office
2. When both ISP routers are connected to the same LAN segment at the top of the tree.

In case 1, the subscriber has a primary ISP connection and a secondary connection used for a limited special purpose. (e.g. for work VPN, video network, etc.). Devices connected under the secondary network router access the Internet through the secondary ISP. All devices still have access to all network resources in the home. Devices under the secondary connection can use the primary ISP if the secondary fails, but other devices do not use the secondary ISP.



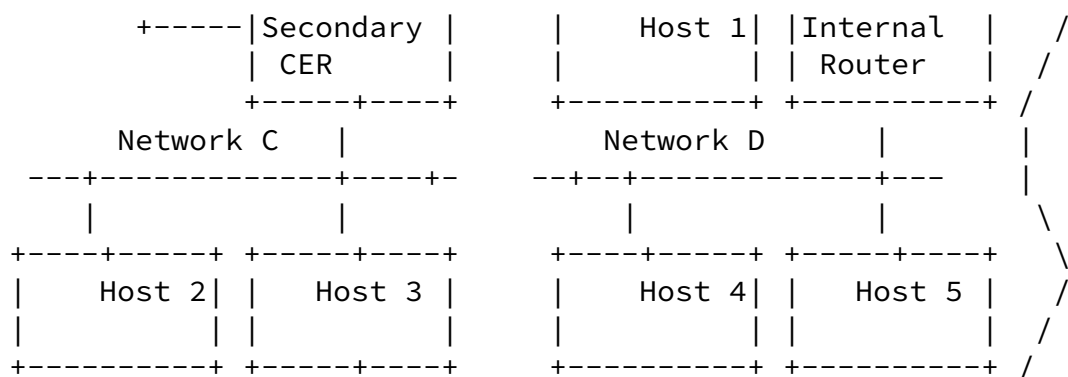


Figure 2: An Example of a multihomed End-User Network

As described above, the primary CER performs prefix sub-delegation to create the hierarchical tree network. The secondary edge router then obtains a second prefix from ISP2 and advertises the ISP2 prefix as part of its RA. The Secondary CER thus includes sub-prefixes from both ISPs in all IA_PD messages to downstream routers with the same "router id.". In a change from the single-homing (or backup router) case, the secondary CER points its default route to ISP2, and adds an internal /48 route to its upstream internal router (e.g. R1). Devices below the the secondary CER (e.g. Host 2, Host 3) use ISP2, but have full access to all internal devices using the ISP1 prefix (and/or ULAs). If the ISP2 link fails, the secondary CER points its default route 'up' and traffic flows to ISP1. Devices not below the secondary CER (e.g. Hosts 1, 4, 5) use ISP1, but have full access to all internal devices using the ISP1 prefix (or ULAs).

In case 2, the secondary CER is installed on the same LAN segment as the primary CER. As above, it acquires a prefix from both the CER and secondary ISP. Since it is on the same LAN segment as the CER, the secondary CER does not delegate prefixes to that interface via DHCP. However, it does generate an RA for the ISP2 prefix on the LAN.

As described above, downstream routers receiving the secondary CER RA acquire an address using SLAAC and generate a prefix for sub-

delegation by prepending the secondary CER prefix with the router ID generated during the receipt of the prefix from the CER. Such routers then generate their own RAs on downstream interfaces and include the secondary prefix as an IA_PD option in future prefix

delegations.

[6.2.1.](#) Multihoming Requirements

MH-1: HIPnet routers configured for active multi-ISP support MUST support DHCP address/prefix acquisition (per [\[I-D.ietf-v6ops-6204bis\]](#) on two interfaces (their WAN and upstream LAN interfaces).

MH-2: HIPnet routers configured for active multi-ISP support MAY route packets based on the source IP address of incoming packets using [\[RFC6724\]](#) logic. This allows traffic sourced from the first ISP prefix to be directed to the first ISP, and traffic sourced from the second ISP prefix to be directed to the second ISP.

MH-3: HIPnet routers configured for active multi-ISP support MUST advertise RAs for prefixes on all interfaces except the one from which the prefix was acquired or one directly attached to a Service Provider network.

[7.](#) Multicast Support

[7.1.](#) Service Discovery

There are several common service discovery protocols such as mDNS [\[RFC6762\]](#)/DNS-SD [\[RFC6763\]](#) and SSDP [\[SSDP\]](#). In a multirouter network, service discovery needs to work across the entire home network (e.g. site-scoped rather than link-scoped). This requires that HIPnet routers forward relevant multicast traffic appropriately, to enable service discovery across the home network.

[7.2.](#) Multicast Proxy Support

In addition to multicast support for service discovery, it is recommended that HIPnet routers support external multicast traffic.

[7.3.](#) Multicast Requirements

MULTI-1: A HIPnet router MUST discard IP multicast packets that fail a Reverse Path Forwarding Check (RPFC).

MULTI-2: A HIPnet router that determines itself to be at the edge of a home network (e.g. via CER_ID option, /48 verification, or other mechanism) MUST NOT forward IPv4 administratively scoped (239.0.0.0/8) packets onto the WAN interface.

MULTI-3: HIPnet Routers MUST forward IPv4 Local Scope multicast packets (239.255.0.0/16) to all LAN interfaces except the one from which they were received.

MULTI-4: A HIPnet router that determines itself to be at the edge of a home network (e.g. via CER_ID option, /48 verification, or other mechanism) MUST NOT forward site-scope (FF05::) IPv6 multicast packets onto the WAN interface.

MULTI-5: HIPnet routers MUST forward site-scoped (FF05::/16) IPv6 multicast packets to all LAN interfaces except the one from which they were received.

MULTI-6: A home router MAY discard IP multicast packets sent between Down Interfaces (different VLANs).

MULTI-7: HIPnet routers SHOULD support an IGMP/MLD proxy, as described in [\[RFC4605\]](#).

[8.](#) Firewall Support

In a home network, routers need to be equipped with stateful firewall capabilities. Home routers will need to provide "on by default" security where incoming traffic is limited to return traffic resulting from outgoing packets. They also need to allow users to create inbound 'pinholes' for specific purposes, such as online gaming, manually similar to those described in Simple Security ([\[RFC6092\]](#)). "Advanced Security" [\[I-D.vyncke-advanced-ipv6-security\]](#) features optionally could be added to provide intrusion detection (IDS/IPS) support.

Local Network Protection for IPv6 [\[RFC4864\]](#) recommends firewall functions that replace NAT security and calls for simple security. Simple Security [\[RFC6092\]](#) defines firewall filtering rules for IPv6 traffic. Advanced Security [\[I-D.vyncke-advanced-ipv6-security\]](#) supports the concept of end-to-end IPv6 reachability and uses adaptive filtering based on Intrusion Prevention System (IPS) functions.

It is recommended that the CER enable a stateful [\[RFC6092\]](#) firewall by default. IRs have three options described below:

IR Firewall Option 1 - Filtering Disabled: Once a home router determines that it is not the CER, it disables its firewall and allows all traffic to pass. The advantages of this approach are that it is simple and easy to troubleshoot and it facilitates whole-home service discovery and media sharing. The disadvantages are that it does not protect home devices from each other (e.g. infected machines could affect entire home network).

IR Firewall Option 2 - Simple Security + PCP: Home routers have a [\[RFC6092\]](#) firewall on by default, regardless of CER/IR status but IRs allow "pin-holing" using PCP [\[RFC6887\]](#). CERs can restrict opening PCP pinholes on the up interface. The advantages of this approach are that it protects the home network from internal threats in other LAN segments and it mirrors legacy IPv4 router behavior. The disadvantages to this approach are that it is less predictable; it relies on application "pin-holing", a "default deny" rule that may interfere with service discovery and/or content sharing, and requires PCP clients (e.g. on PCs and CPE devices).

IR Firewall Option 3 - Advanced Security: Once a home router determines that it is not the CER, it disables its [\[RFC6092\]](#) firewall but activates an [\[I-D.vyncke-advanced-ipv6-security\]](#) firewall (IPS). The advantages to this approach are that it protects the home network from internal threats in other segments and is more predictable than Option 2, since internal traffic is allowed by default. The disadvantages are that adaptive filtering is more complex than static filtering and typically requires a "fingerprint" subscription to work well.

It is recommended that dual-stack routers configure IPv4 support to mirror IPv6, as described above.

While this section describes default router behavior, device manufacturers are encouraged to make router security options user-configurable.

[8.1.](#) Requirements

SEC-1: The CER MUST enable a stateful [\[RFC6092\]](#) firewall by default.

SEC-2: HIPnet routers MUST only perform IPv4 NAT when serving as the CER.

SEC-3: By default, HIPnet routers SHOULD configure IPv4 firewalling rules to mirror IPv6.

SEC-4: HIPnet routers serving as CER SHOULD NOT enable UPnP IGD ([\[UPnP-IGD\]](#)) control by default.

Grundemann, et al.

Expires January 13, 2014

[Page 17]

Internet-Draft

[draft-grundemann-hipnet](#)

July 2013

[9.](#) Running Code

The HIPnet architecture described in this document was successfully demonstrated to work at Bits-N-Bytes in Orlando during IETF 86. The proof-of-concept software was simply a version of [\[OpenWRT\]](#) modified for HIPnet compliance by a small team of undergrads from the University of Colorado, Boulder. You can download the prototype/proof-of-concept software from [\[HIPnetPoC\]](#).

[10.](#) IANA Considerations

This document makes no request of IANA.

Note to RFC Editor: this section may be removed on publication as an RFC.

[11.](#) Security Considerations

Security considerations are discussed in the Firewall Support section above.

[12.](#) Acknowledgements

TBD

[13.](#) References

[13.1.](#) Normative References

[I-D.ietf-v6ops-6204bis]

Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", [draft-ietf-v6ops-6204bis-12](#) (work in progress), October 2012.

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", [RFC 3315](#), July 2003.
- [RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", [RFC 3633](#), December 2003.

Grundemann, et al.

Expires January 13, 2014

[Page 18]

Internet-Draft

[draft-grundemann-hipnet](#)

July 2013

- [RFC4605] Fenner, B., He, H., Haberman, B., and H. Sandick, "Internet Group Management Protocol (IGMP) / Multicast Listener Discovery (MLD)-Based Multicast Forwarding ("IGMP /MLD Proxying")", [RFC 4605](#), August 2006.
- [RFC4864] Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", [RFC 4864](#), May 2007.
- [RFC6092] Woodyatt, J., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 Internet Service", [RFC 6092](#), January 2011.

[13.2](#). Informative References

[HIPnetPoC]

CableLabs, "HIPnetPoC", July 2013, <http://www.cablelabs.com/cablemodem/ri/hipnet_prototype.html>.

[I-D.chakrabarti-homenet-prefix-alloc]

Nordmark, E., Chakrabarti, S., Krishnan, S., and W. Haddad, "Simple Approach to Prefix Distribution in Basic Home Networks", [draft-chakrabarti-homenet-prefix-alloc-01](#) (work in progress), October 2011.

- [I-D.donley-dhc-cer-id-option]
Donley, C. and C. Grundemann, "Customer Edge Router Identification Option", [draft-donley-dhc-cer-id-option-01](#) (work in progress), September 2012.
- [I-D.grundemann-homenet-hipnet]
Grundemann, C., Donley, C., Brzozowski, J., Howard, L., and V. Kuarsingh, "A Near Term Solution for Home IP Networking (HIPnet)", [draft-grundemann-homenet-hipnet-01](#) (work in progress), February 2013.
- [I-D.ietf-homenet-arch]
Chown, T., Arkko, J., Brandt, A., Troan, O., and J. Weil, "Home Networking Architecture for IPv6", [draft-ietf-homenet-arch-08](#) (work in progress), May 2013.
- [I-D.vyncke-advanced-ipv6-security]
Vyncke, E., Yourtchenko, A., and M. Townsley, "Advanced Security for IPv6 CPE", [draft-vyncke-advanced-ipv6-security-03](#) (work in progress), October 2011.
- [OpenWRT] OpenWRT, "OpenWRT", July 2013, <<http://openwrt.org/>>.

Grundemann, et al. Expires January 13, 2014 [Page 19]

Internet-Draft [draft-grundemann-hipnet](#) July 2013

- [RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", [BCP 5](#), [RFC 1918](#), February 1996.
- [RFC2131] Droms, R., "Dynamic Host Configuration Protocol", [RFC 2131](#), March 1997.
- [RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", [RFC 4861](#), September 2007.
- [RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", [RFC 6724](#), September 2012.
- [RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", [RFC 6762](#), February 2013.
- [RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service

Discovery", [RFC 6763](#), February 2013.

[RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", [RFC 6887](#), April 2013.

[SSDP] UPnP Forum, "SSDP", October 2008, <<http://www.upnp.org/>>.

[UPnP-IGD] UPnP Forum, "UPnP-IGD", November 2001, <<http://www.upnp.org/>>.

Authors' Addresses

Chris Grundemann
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA

Phone: +1-303-351-1539
Email: c.grundemann@cablelabs.com

Grundemann, et al.

Expires January 13, 2014

[Page 20]

Internet-Draft

[draft-grundemann-hipnet](#)

July 2013

Chris Donley
CableLabs
858 Coal Creek Circle
Louisville, CO 80027
USA

Email: c.donley@cablelabs.com

John Jason Brzozowski
Comcast Cable Communications
1306 Goshen Parkway

Chester, PA 19380
USA

Email: john_brzozowski@comcast.com

Lee Howard
Time Warner Cable
13241 Woodland Park Rd
Herndon, VA 20171
USA

Email: william.howard@twcable.com

Victor Kuarsingh
Rogers Communications
8200 Dixie Road
Brampton, ON L6T 0C1
Canada

Email: victor.kuarsingh@rci.rogers.com