8. RFC 7368： IPv6 Home Networking Architecture Principles
RFC 7368： IPv6 家庭網路架構原則

網際網路工程任務組(IETF)
Request for Comments：7368
分類：標準
ISSN：2070-1721

T. Chown Ed.
南安普敦大學
J. Arkko
愛立信
A. Brandt
Sigma 設計
O. Troan
思科系統公司
J. Weil
時代華納有線

2014 年 10 月

IPv6 家庭網路架構原則

摘要

本文描述了住宅家庭網路中不斷發展的網路技術，其中設備數量越來越多，內部路由越來越多。
本文的目標是定義基於 IPv6 的家庭網路的通用架構，描述相關的原則，注意事項和要求。
本文簡要強調了 IPv6 引入家庭網路的具體含義，討論了該架構的各個要素，並建議瞭如何在家庭網路中採用標準的 IPv6 機制和定址。
該體系結構描述了對特定附加功能的特定協定擴充的需求。
假設 IPv6 家庭網路不是主動管理的，並且作為僅 IPv6 或雙堆疊網路運行。本文中沒有針對網路的 IPv4 部分的建議。

本文的狀態

本文並不是一個網際網路標準協定規範; 其出版是為了提供訊息。

本文是網際網路工程任務組（IETF）的產品。 它代表了 IETF 社群的共識。 它已經過公眾審查，並已獲得網際網路工程指導小組

（IESG）的批准發布。 並非所有 IESG 批准的文件都適用於任何級別的網際網路標準; 請參閱 RFC 5741 的第 2 部分。

有關本文當前狀態、勘誤以及如何提供反饋訊息，請訪問 http://www.rfc-editor.org/info/rfc7368

目錄

1. 前言

本文重點介紹住宅家庭網路中不斷發展的網路技術，其中設備數量不斷增加，內部路由增加的趨勢以及部署和營運相關的挑戰。家庭網路通過越來越廣泛的設備和媒體擴散網路技術的趨勢越來越明顯。
規模和多樣性的演變在 IETF 協定設定了條件。 其中一些要求涉及 IPv6 的引入，而其他要求涉及引入家庭自動化和傳感器的專用網路。

雖然在編寫時存在一些複雜的家庭網路拓撲，但大多數是相對簡單的單子網路，並且表面上僅使用 IPv4 進行操作。 雖然網路內可能存在 IPv6 流量，例如，用於服務發現，但是由 ISP 提供家庭網作為 IPv4 網路。 此類網路通常還採用應避免的解決方案，例如使用（級聯）網路地址轉換（NAT）[RFC3022]進行私有[RFC1918]定址，或者它們可能需要專家協助才能進行設置。

相比之下，新興的支援 IPv6 的家庭網路很可能具有多個內部子網，例如，便於私有和訪客網路，異構鏈路層和智慧電網組件，並且具有足夠的地址空間可用於允許每個設備具有全局獨特的地址。這意味著需要內部路由功能，並且家庭網路的 ISP 委派足夠大的位址塊，以允許為家庭網路中的每個子網分配前綴。

期望家庭用戶配置他們的網路是不切實際的。因此，該文件的假設是家庭網路盡可能地自組織和自我配置，即，它應該在沒有住宅用戶的主動管理的情況下運行。

本文中的體系結構主要關注於在引入 IPv6 時要解決的問題，著眼於比我們今天使用 IPv4 更好的結果，以及旨在提供更一致的解決方案，以滿足許多已確定的要求盡可能。本文旨在為家庭網路中如何使用標準 IPv6 機制和定址[RFC2460] [RFC4291]提供基礎和指導原則，同時與現有的 IPv4 機制共存。在新興的雙堆疊家庭網路中，引入 IPv6 對 IPv4 操作沒有不利影響至關重要。我們假設家庭網路中的 IPv4 網路架構就是這樣，並且不能通過新建議進行修改。本文未討論 IPv4 家庭網路如何提供或提供對多個子網的支援。不應該假設任何未來使用 IPv6 創建的新功能將向後兼容以包括 IPv4 支援。
此外，未來的部署或在其他雙堆疊家庭網路內的特定子網可能僅僅是 IPv6，在這種情況下，IPv4 影響的考慮將不適用。

本文提出了一種基線家庭網路體系結構，使用盡可能經過驗證和可靠的協定和實現。 本文的範圍主要是網路層技術，它們提供了實現定址，連接，路由，命名和服務發現的基本功能。
例如，雖然它可能表明家庭網路組件必須易於部署和使用，但它不討論特定的用戶界面，也不討論特定的物理，無線或數據鏈路層考慮因素。 同樣，我們也沒有從上到下指定整個家庭網路路由器的設計; 相反，我們專注於第 3 層方面。 這意味著第 2 層很大程度上超出了範圍，我們假設存在支援 IPv6 的資料鏈路層，並且我們會做出相應的反應。 任何 IPv6-over-Foo 定義都在其他地方發生。

已淘汰[RFC6204]的[RFC7084]定義了客戶邊緣（CE）路由器的基本要求。 此更新包括 CE 路由器上特定轉換工具的要求定義，特別是 Dual-Stack Lite（DS-Lite）[RFC6333]和 IPv4 基礎架構上的 IPv6 快速部署（第 6 版）[RFC5969]。 CE 路由器設備的這種詳細規範被認為超出了該體系結構文件的範圍，並且我們假設採用該體系結構的 CE 路由器設備規範的任何所需更新將作為對這些現有文件的單獨且特定的更新來處理。 此外，本文的範圍是內部主網，因此 CE 路由器的 WAN 側的特定功能超出了本文的範圍。

1.1. 術語和縮語

在本節中，我們定義了整個文本中使用的術語和縮寫。

- 邊界(Border)：通常駐留在路由器上的點，在兩個網路之間，例如在主內部主網和訪客網路之間。 這定義了可以應用針對不同類型的流量的過濾和轉發策略的點。

- CE 路由器(CE router)：客戶邊選路器。 用於家庭網路的邊界路由器。 CE 路由器將家庭網路連接到服務提供商網路。

- FQDN：完全合格的域名。全球唯一的名稱。

- 訪客網路(Guest network)：家庭網路的一部分，供訪客或訪客使用（家庭網路）。訪客網路上的設備通常可能看不到或無法使用家庭中的所有服務（網路）。

- Homenet：家庭網路，包括主機和路由器設備，一個或多個 CE 路由器提供與服務提供商網路的連接。

- ISP：網際網路服務提供商。 提供網際網路訪問的實體。 在本文中，服務提供商專門使用 IPv6 提供網際網路訪問，並且還可以提供 IPv4 網際網路訪問。服務提供商可以通過各種不同的傳輸方法提供這種訪問，例如 DSL，電纜，無線等。

- LLN：低功耗和有損網路。

- LQDN：本地限定域名。 家庭網路的本地名稱。

- NAT：網路地址轉換。 通常是指 IPv4 網路地址端口轉換（NAPT）[RFC3022]。

- NPTv6：IPv6 到 IPv6 網路前綴轉換[RFC6296]。

- PCP：端口控制協定[RFC6887]。

- 領域(Realm)：由定義的邊框分隔的網路。 家庭網路中的訪客網路可以形成一個領域。

- '簡單安全'('Simple Security')：在[RFC4864]中定義，並在[RFC6092]中進一步擴充;描述了IPv6網路的推薦周邊安全功能。

- ULA：IPv6唯一本地地址[RFC4193]。

- VM：虛擬機。

2. IPv6對家庭網路的影響

雖然 IPv6 在很多方面類似於 IPv4，但它通常可以部署的方式存在一些顯著差異。它改變了地址分配原則,使多址定址成為常態，並且通過大大增加的地址空間,它允許全球唯一的IP地址用於家庭網路中的所有設備。 本節概述了為家庭網路引入 IPv6 的一些關鍵影響，這些影響同時既有前途又有問題。

2.1. 多個子網和路由器

雖然在家庭網路中優選涉及盡可能少子網的簡單第3層拓撲，但由於各種原因，專用（路由）子網的合併仍然是必要的。例如，現代家庭路由器中越來越常見的特徵是支援客戶和專用網路子網的能力。同樣地,可能需要將主家庭自動化或公司擴充LAN(其中家庭工作者可以使用虛擬專用網路將其公司網路擴充到家中，通常作為乙太網路設備上的一個端口）從主要網路接入中分離出來。網路或不同的子網通常可以與具有不同路由和安全策略的家庭網路的部分相關聯。此外，隨著網路開始採用傳統乙太網路技術和為低功耗和有損網路（LLN）設計的鏈路層（例如用於某些類型的傳感器設備的鏈路層),鏈路層網路技術將變得更加異構。因此，限制從乙太網路鏈接到具有較低容量的鏈路的流量成為一個重要的主題。

為家庭網路引入IPv6使得每個家庭網路都可以從其ISP委派足夠的地址空間，為家庭中的每個這樣的子網提供全球唯一的前綴。雖然標準/ 64 IPv6前綴中的地址數實際上是無限的，但可用於分配給家庭網路的前綴數量不是。 結果，家庭網路的生長抑製劑從地址數轉移到提供者提供的前綴數; BCP 157 [RFC6177]中討論了

這個主題,它建議"終端站點始終能夠為其實際和計劃使用獲得合理數量的地址空間"。

2.2. 全球定址能力和消除 NAT

通過引入 IPv6 來恢復網際網路上直接端到端通信的可能性,一方面是創新和簡化網路營運的難以置信的機會,但另一方面,它也是一個問題。它可能會使內部網路中的節點暴露於從網際網路所接收的不需要和可能為惡意的流量。

由於設備和應用程序在具有全局唯一地址時能夠直接相互通信,因此可能期望提高主機安全性以補償這一點。應該注意的是,許多設備可能(例如)附帶默認設置,如果全局可訪問,它們很容易受到外部攻擊者的攻擊,或者它們可能根本不能設計健全,因為假設這些設備只是在專用網路上使用或設備沒有計算能力來應用必要的安全方法。此外,設備(或其韌體)的升級週期可能很慢和/或缺少自動更新機制。

因此,區分可定址性和可達性是很重要的。 雖然 IPv6 通過在家中使用全球唯一地址來提供全局可定址性,但是設備是否可全局訪問將取決於任何防火牆或過濾配置,而不是像 IPv4 的情況那樣,NAT 的存在或使用。 在這方面,IPv6 網路可以或可以不在其邊界處應用過濾器來控制這種業務,即在家庭網路 CE 路由器處。[RFC4864]和[RFC6092]討論了這種過濾以及針對發佈到家庭網路中的外部流量的"默認拒絕"策略的"默認允許"的優點。第 3.6.1 節將進一步討論該主題。

2.3. 設備的多址解調

在 IPv6 網路中,設備通常將獲取多個地址,通常至少是鏈路本地地址和一個或多個全局唯一地址(GUA)。在家庭網路是多宿主的情況下,設備通常從每個上游 ISP 的委託前綴內接收 GUA。如果網路是雙堆疊,IPv6 唯一本地地址(ULA)[RFC4193](見下文),以及一個或多個 IPv6 隱私地址[RFC4941],則設備也可以具有 IPv4 地址。

因此，應該認為 IPv6 家庭網路上的設備是多址的並且需要針對任何給定連接對候選源和目的地地址對做出適當的地址選擇決策。在多歸屬方案中，節點將配置來自每個上游 ISP 前綴的一個地址。在這種情況下，BCP 38 [RFC2827]中描述的上游入口過濾的存在要求這樣的多址節點選擇用於相應上行鏈路的正確源地址。 IPv6 [RFC6724]的默認地址選擇為此提供了解決方案，但這裡的一個挑戰是節點可能沒有基於地址單獨做出決策所需的訊息。我們在 3.2.4 節討論這個挑戰。

2.4. 獨特的本地地址（ULAs）

[RFC4193]定義了 IPv6 的 ULA，可用於定址單個站點範圍內的設備。 [RFC7084]中描述了對 IPv6 CE 路由器的 ULA 的支援。運行 IPv6 的家庭網路應該將 ULA 與其全局唯一前綴一起部署，以允許家庭網路內的設備（在不同子網上）之間的穩定通信，其中外部分配的全局唯一前綴可以隨時間改變，例如，由於在訂戶內的重新編號。 ISP，或外部連接可能暫時不可用的地方。 使用提供商分配的全局地址的家庭網路暴露給其 ISP 重新編號網路的程度比以前大得多，而對於 IPv4，NAT 在一定程度上隔離了用戶對 ISP 的重新編號。

在建立網路時，可能存在沒有外部連接的時期，在這種情況下，子網間通信需要 ULA。 在家庭自動化網路正在新家庭/部署中建立的情況下（早在家庭建設期間），這樣的網路可能需要使用他們自己的/ 48 ULA 前綴。根據家庭網路所有者無法控制的情況，可能無法重新編號家庭自動化網路使用的 ULA，因此可能需要在 ULA / 48 之間進行路由。 此外，一些設備（尤其是受限制設備）可能僅具有 ULA（除了本地鏈路之外），而其他設備可以具有 GUA 和 ULA。

請注意，與 RFC 1918 中描述的私有 IPv4 空間不同，使用 ULA 並不意味著使用 IPv6 等效的傳統 IPv4 NAT [RFC3022]或基於 NPTv6 前綴的 NAT [RFC6296]。 當 homenet 中的 IPv6 節點同時具有 ULA 和全局唯一 IPv6 地址時，它應僅在內部使用其 ULA 地址，並使用其附加的全局唯一 IPv6 地址作為外部通信的源地址。這應該是支援 IPv6 [RFC6724]的默認地址選擇"的自然行為。 通過在遠程網路中的主機和設備之間使用這種全球唯一地址，避免

了 NAT 或 NPTv6 轉換的架構成本和復雜性，尤其是應用的複雜性。因此,建議不要在家庭網路架構中使用 IPv6 NAT 和 NPTv6。此外，家庭網路邊界路由器應過濾具有 ULA 源/目的地址的資料封包，如第 3.4.2 節所述。

家庭網路中的設備可以僅被給予 ULA 作為限制來自家庭網路之外的可達性的手段。 默認情況下，ULA 可以用於沒有附加配置（例如，通過 web 接口）的設備，它們僅向內部網路提供服務。例如，打印機可能只接受 ULA 上的傳入連接，直到配置為全局可達，此時它獲取全局 IPv6 地址，並可通過全局名稱空間進行宣告。

在使用 ULA 和全局前綴的情況下，ULA 源地址用於在適當時與 ULA 目的地地址通信，即當 ULA 源和目的地位於已知在同一家庭網路內使用的/ 48 ULA 前綴內時。
在單個家庭網路中使用多個/ 48 個 ULA 前綴的情況下（可能是因為多個家庭網路路由器各自獨立地自動生成/ 48 ULA 前綴然後共享前綴/路由訊息），利用 ULA 源地址和 ULA 目的地地址 來自兩個不相交的內部 ULA 前綴比使用 GUA 更可取。

雖然家庭網路應該在啟用兩個或更多/ 48 個 ULA 的情況下正常運行，但是為了解決一致性和策略實施，需要一種用於創建和使用單個/ 48 ULA 前綴的機制。

使用 ULA 的一個反駁論點是，不要為了暫時失去連接而積極地棄用全局前綴，因此，如果主機丟失其全局地址，則必須存在比租期更長的連接斷開，即便如此，在沒有連接時棄用前綴可能不可取。但是，在此體系結構中假設 homenet 應支援和使用 ULA。

2.5. 避免手動配置 IP 地址

一些 IPv4 家庭網路設備向用戶公開 IPv4 地址，例如，可以通過 web 接口配置的家庭 IPv4 CE 路由器的 IPv4 地址。在潛在復雜的未來 IPv6 家庭網路中，不應期望用戶在設備或應用程序中輸入 IPv6 文字地址，因為它們具有更大的長度以及這種地址對典型家庭用戶的明顯隨機性。 因此，即使對於最簡單的功能，簡單命名

和相關的（最小的，理想情況下零配置）服務發現對於簡單地部署和使用家庭網路設備和應用程序也是必不可少的。

2.6. 僅 IPv6 操作

可能首先在新的家庭網路部署中部署僅 IPv6 的網路，通常稱為“綠地”場景，其中沒有現有的 IPv4 功能，或者可能作為雙堆疊網路的一個元素。 僅運行 IPv6 會增加額外的要求，例如，設備通過 IPv6 傳輸獲取配置訊息（不依賴於 IPv4 協定，例如 IPv4 DHCP），以及設備能夠啟動與僅 IPv4 的外部設備的通信。

在[RFC7084]中討論了可以由家庭網路 ISP 部署的一些特定過渡技術。 另外，在 CE 路由器上可能需要某些其他功能，例如，為了訪問 IPv4 因特網中的內容，NAT64 [RFC6144]和 DNS64 [RFC6145]可能是適用的。

針對這些類型的需求的廣泛可用性將有助於加速僅使用 IPv6 的家庭網路。 但是，這些細節超出了本文的範圍，特別是那些駐留在 CE 路由器上的函數。

3. 家庭網路架構原則

本文的目的是概述如何使用標準 IPv6 定址和協定[RFC2460] [RFC4291]作為基礎，構建涉及多個路由器和子網的高級基於 IPv6 的家庭網路。 如 3.1 節所述，解決方案應盡可能重用現有協定並儘量減少對主機和路由器的更改，但可能需要一些新的協定或擴充。 在本節中，我們將討論所提出的家庭網路架構的元素，並討論相關的設計原則。

通常，家庭網路設備需要能夠在具有一系列不同屬性和拓撲的網路中操作，其中家庭用戶可以以任意方式將組件插入在一起並期望所得到的網路運行。 考慮到典型家庭用戶的知識水平，重要的手動配置很少（如果有的話）可能甚至是可取的。 因此，網路應盡可能自我配置，但不應排除高級用戶的配置。

家庭網路需要能夠處理或提供至少以下內容：

- 路由
- 路由器的前綴配置
- 名稱解析
- 服務發現
- 網路安全

本文的其餘部分描述了家庭網路體系結構可以提供這些屬性的原則。

3.1. 總則

由於策略或鏈路層兼容性原因，網際網路標準社群幾乎無法對物理拓撲或某些網路在網路層分離的需求做些什麼。但是，使用 IP 定址和網路互連機制有很大的靈活性。本文討論瞭如何使用這種靈活性來提供最佳用戶體驗，並確保網路在未來可以通過新應用程序發展。在設計家庭網路協定解決方案時，應遵循本文中描述的原則。

3.1.1. 重用現有協定

現有協定將用於滿足家庭網路的要求。必要時，將對這些協定進行擴充。當沒有現有協定被發現是合適的，可以使用一個新的或新興的協定。因此，重要的是不要做出任何會妨礙使用新的或新興協定的設計或架構決策。

一種通常保守的方法，優先考慮運行（和可用）代碼。在需要新協定的地方，非常需要有適當供應商或開發社群承諾實施的證據。使用的協定應該向後兼容，並且在進行更改時向前兼容。

3.1.2. 最小化對主機和路由器的變更

為了最大化新主網的可部署性，應盡可能減少對主機和路由器的任何更改要求; 然而，例如，通過主機或路由器改變逐步提高能力的解決方案可能是可接受的。可能存在無法避免更改的情況，

例如，允許給定的家庭網路路由協定自我配置或支援基於源地址以及目標地址的路由(以改進多宿主支援,如第 3.2.4 節中所述)。

3.2. 家庭網路拓撲

本節將考慮家庭網路拓撲以及可能在設計架構時應用的原則，以支援盡可能廣泛的此類拓撲。

3.2.1. 支援任意拓撲

理想情況下，家庭網路中的拓撲應該沒有內置的假設，因為用戶能夠以“巧妙”的方式連接他們的設備。 因此，需要支援任意拓撲和任意路由，或者至少用戶犯錯誤時的故障模式應該盡可能健壯，例如，停用基礎設施的某個部分以允許其餘部分操作。 在這種情況下，理想情況下，用戶應該對遇到的故障模式有一些有用的指示。

除非用戶在拓撲中創建物理島，否則不應存在導致連接丟失的拓撲方案。可以創建的一些潛在病理案例包括將路由器的端口橋接在一起; 但是，這種情況可以由路由器檢測和處理。 路由拓撲中的循環在某種意義上是好的，因為它們提供冗餘。 包含潛在橋接環路的拓撲結構可能很危險，但當交換機在另一個接口上學習其中一個接口的媒體訪問控制（MAC）地址或運行生成樹或鏈路狀態協定時，也可以檢測到這些拓撲。 只有具有這種潛在環路的拓撲結構才能使用真正病態的簡單中繼器。

由於設備的添加或移除，以及臨時故障或連接問題，家庭網路的拓撲結構可能隨時間而變化。 在某些情況下可能導致，例如，多宿主家庭網路被分成兩個孤立的家庭網路，或者在糾正了這樣的故障之後，兩個孤立的部分重新配置回單個網路。

3.2.2. 網路拓撲模型

如上所述，雖然架構可能關注可能的常見拓撲，但它不應排除任何構造的任意拓撲。

在撰寫本文時，大多數 IPv4 家庭網路模型往往相對簡單，通常是 ISP 的單個 NAT 路由器和單個內部子網，但如前所述，網路體系結構的演變正在推動更複雜的拓撲，例如分離 客人和私人網路。可能還有一些級聯的 IPv4 NAT 場景，我們將在下一節中提到。對於 IPv6 家庭網路，[RFC7084]中描述的網路體系結構至少應受支援。

我們可以使用家庭網路的許多屬性或屬性來描述其拓撲和操作。以下屬性適用於任何 IPv6 家庭網路：

- 存在內部路由器。家庭網路可以具有一個或多個內部路由器，或者可以僅從 CE 路由器上的接口提供子網。

- 存在孤立的內部子網。 可能存在隔離的內部子網，它們之間沒有直接連接（每個子網都有自己的外部連接）。 隔離可以是物理的，也可以通過 IEEE 802.1q VLAN 實現。 然而，後者不是典型用戶期望配置的東西。

- CE 路由器的劃分。 CE 路由器可以由 ISP 管理，也可以不由 ISP 管理。如果分界點是客戶可以提供或管理 CE 路由器，則其配置必須簡單。 必須支援這兩種模型。

各種形式的多宿主可能在 IPv6 歸屬網路中變得更普遍，其中歸屬網路可以具有兩個或更多個外部ISP連接，如下面進一步討論的。因此，對於此類網路，還應考慮以下屬性：

- 上游提供商的數量。如今，大多數家庭網路都由一個上游 ISP 組成，但未來可能會出現多個 ISP，無論是為了恢復還是提供其他服務。 每個都會提供自己的前綴。 有些可能會或可能不會提供到公共網際網路的默認路由。

- CE 路由器數量。 家庭網可以具有單個 CE 路由器，其可以用於一個或多個提供商，或多個 CE 路由器。 多個 CE 路由器的存在增加了多宿主場景和協定（如 PCP）的額外複雜性，這些協定可能需要在與後續流量流相同的 CE 路由器上管理面向連接的狀態映射。

在以下部分中，我們將舉例說明我們將來可能會看到的家庭網路拓撲的類型。這不是一個詳盡或完整的清單，而是一個便於本文討論的指示性清單。

3.2.2.1. A：單 ISP，單 CE 路由器和內部路由器

圖 1 顯示了具有多個局域網的家庭網路。出於與使用中的不同鏈路層技術或由於策略原因相關的原因，例如一個子網中的經典乙太網路和另一個子網中的 LLN 鏈路層技術，可能需要這些。 在此示例中，沒有單個路由器先驗了解整個拓撲。拓撲本身也可能很複雜，例如，可能無法假設純樹形式（因為家庭用戶可能將路由器插在一起形成任意拓撲，包括那些具有潛在環路的拓撲）。

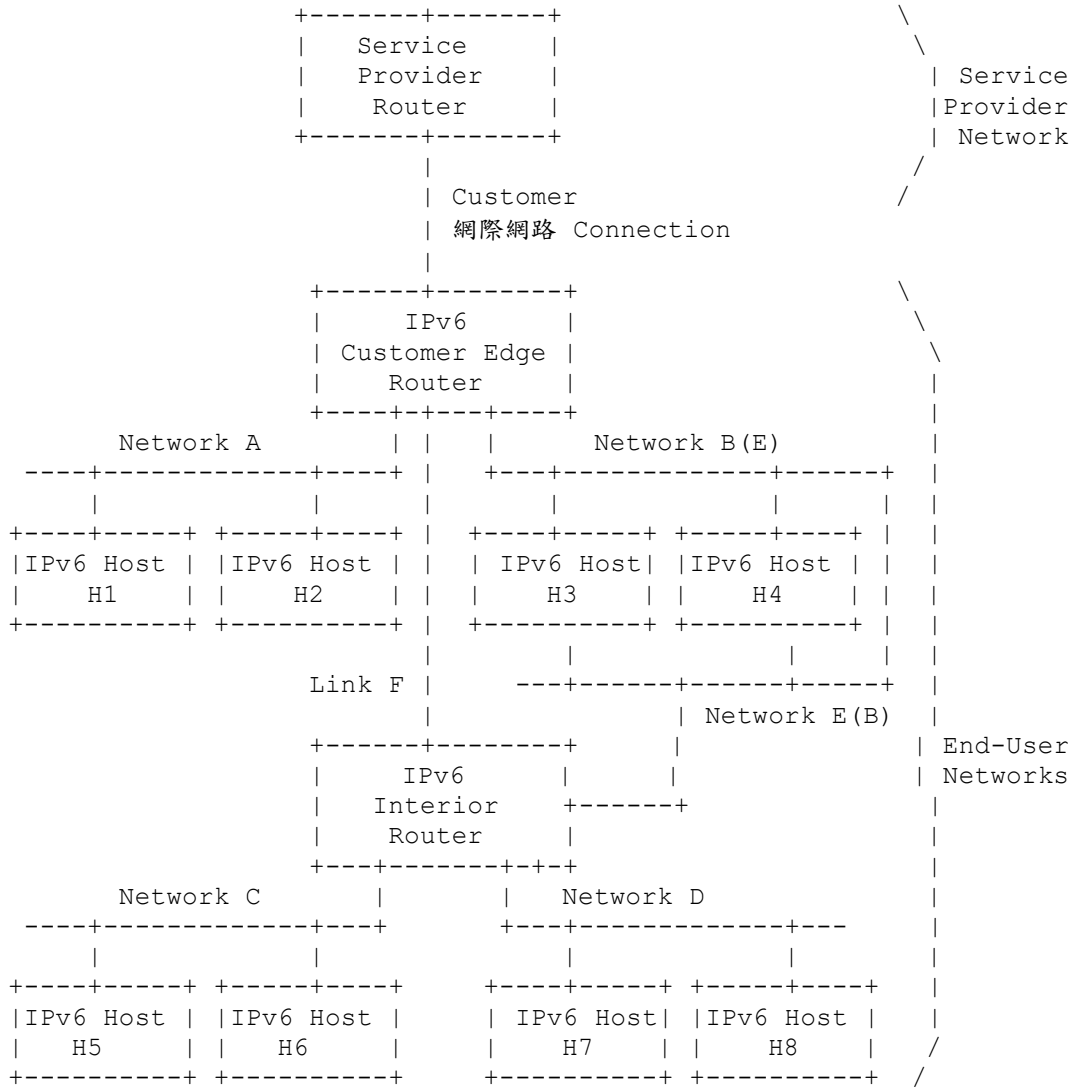

圖 1

在此圖中，有一個 CE 路由器。 它有一個上行鏈路接口。 它有三個附加接口連接到網路 A,鏈路 F 和網路 B.IPv6 內部路由器（IR）有四個接口連接到鏈路 F，網路 C，網路 D 和網路 E.網路 B 和網路 E 已橋接，可能是無意中。這可能是因為在網路 B 的交換機和網路 E 的交換機之間連接了一條線路。

邏輯網路 A 到 F 中的任何一個可以是有線的或無線的。在顯示多個主機的情況下，可能通過 CE 路由器或 IPv6（IR），無線網路上的一個或多個物理端口，或僅通過一個或多個僅為第 2 層的乙太網路交換機。

3.2.2.2. B：兩個 ISP，兩個 CE 路由器和共享子網

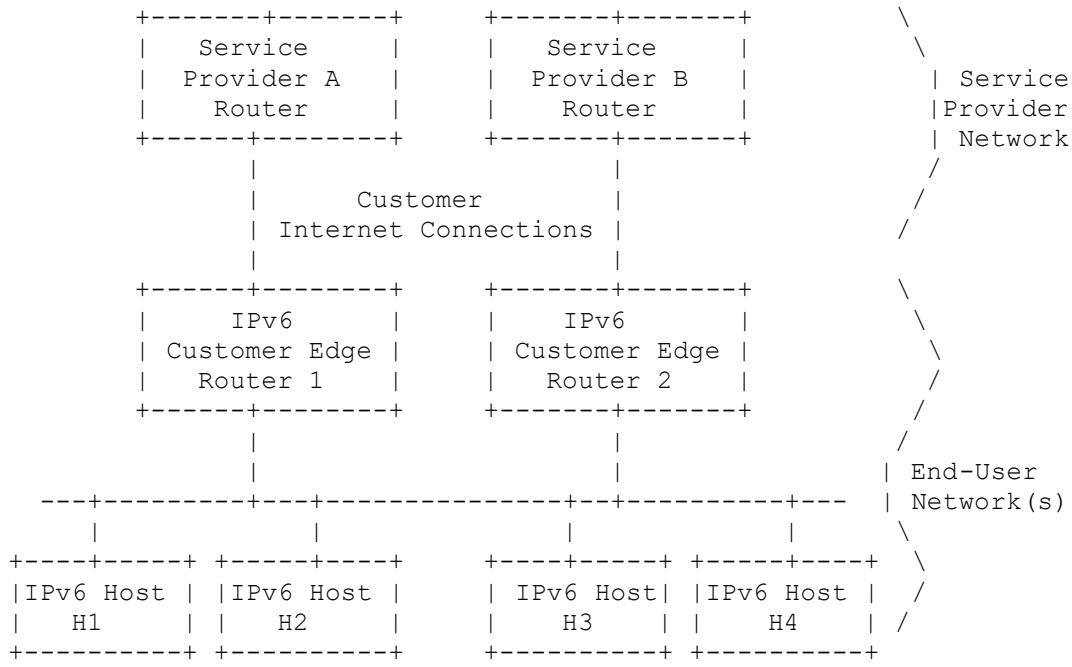

圖 2

圖 2 說明了一個多宿主家庭網模型，其中客戶通過 CE 路由器 1 連接到 ISP A，並通過 CE 路由器 2 連接到 ISP B.此示例顯示了一個共享子網，其中 IPv6 節點可能是多宿主並接收多個 IPv6 全局前綴，一個 每個 ISP。 此模型也可以與圖 1 中所示的模型結合使用，以創建具有多個內部路由器的更複雜的方案。 或者，上述共享子網可以分成兩部分，使得每個 CE 路由器服務於單獨的隔離子網，這是當今一些 IPv4 網路所見的情況。

3.2.2.3. C：兩個 ISP，一個 CE 路由器和共享子網

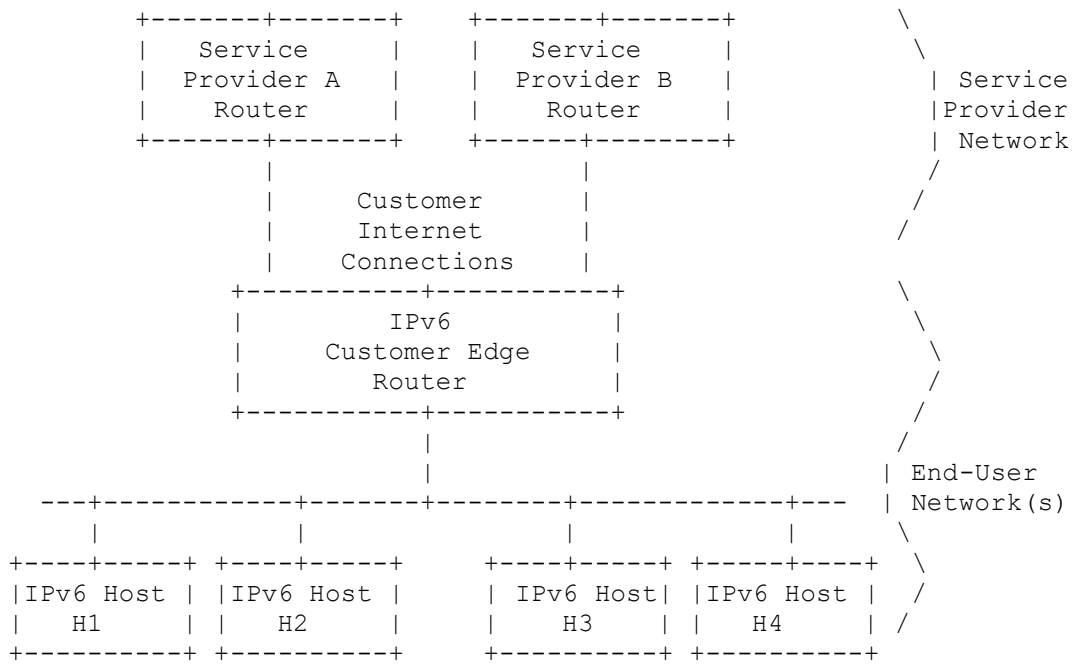

圖 3

圖 3 示出了一種模型，其中家庭網路可以具有到多個提供者的多個連接或具有共享內部子網的到同一提供者的多個邏輯連接。

3.2.3. 雙堆疊拓撲

在不久的將來，預計大多數家庭網路部署將是雙堆疊 IPv4 / IPv6。在這樣的網路中，重要的是不要引入新的 IPv6 功能，如果與 IPv4 + NAT 一起使用會導致故障，因為這種雙堆疊家庭網路在一段時間內是常見的。也就是說，希望 IPv6 在盡可能多的場景中比 IPv4 更好地工作。 此外，家庭網路架構必須在沒有 IPv4 的情況下運行。

一般建議遵循與 IPv4 相同的拓撲結構，但不使用 NAT。 因此，應該使用路由 IPv6，其中使用 IPv4 NAT，並且在沒有 NAT 的情況下，可以使用路由或橋接。與將高速和低速共享媒體橋接在一起相比，路由可能具有優勢，此外，橋接可能不適合某些網路，例如特定行動網路。

在某些情況下，IPv4 家庭網路可能具有級聯 NAT。 最終用戶經常不知道他們已經創建了這樣的網路，因為“家庭路由器”和“家庭交換機”經常混淆。 此外，還有一些情況是 NAT 路由器包含在虛擬機管理程序中或已啟用網際網路連接共享服務的情況下。 本文同樣適用於此類隱藏的 NAT“路由器”。 將需要 IPv6 路由版本的此類案例。 因此，我們應該注意到，家庭網路中的路由器可能不是單獨的物理設備; 它們可能嵌入在其他設備中。

3.2.4. 內送流量備援容錯機制

如上面的網路模型所示，家庭網路可以多宿主到多個提供者。 這可以採用一種形式，其中在家庭中存在多個隔離網路或者更加集成的網路，其中連接選擇需要是動態的。 目前的做法通常是前一種做法，但後者預計會變得更加普遍。

在一般的家庭網路體系結構中，多宿主主機應使用全局 IPv6 地址進行多址定址，該地址來自與其通信或通過的每個 ISP 委派的全局前綴。 當使用這種多址時，主機需要某種方法來選擇連接的源和目標地址對。 主機可以通過各種方法選擇要使用的源地址，最常見的是[RFC6724]。 應用程序當然可以做不同的事情，這不應該被排除在外。

對於上面說明的單個 CE 路由器網路模型 C，可以通過 CE 路由器處的基於源的路由來提供多宿主。 使用多個出口路由器，如在 CE 路由器網路模型 B 中，複雜性增加。 給定在歸屬網路上具有源地址的分組，如果通過錯誤的 ISP 退出，則必須將分組路由到適當的出口以避免入口過濾，如 BCP 38 中所述。 非常希望以最有效的方式將分組路由到正確的出口，但是作為最低要求，不應該丟棄分組。

家庭網路體系結構應該支援上述模型，即一個或多個 CE 路由器。 然而，一般的多歸屬問題很廣泛，迄今為止在 IETF 內提出的解決方案包括用於監視連接性，流量工程，識別符定位器分離，跨多宿事件的連接生存性等的複雜體系結構。 因此，家庭網路架構應盡可能地降低任何多宿主支援的複雜性。

[RFC7157]中記錄了這種“更簡單”方法的一個例子。 或者，泛洪/路由協定可以潛在地用於通過家庭網路傳遞訊息，使得內部路由器和最終終端主機可以學習每個前綴配置訊息，從而允許做出更好的地址選擇決策。 但是，這意味著路由器，並且很可能是主機更改。 另一種途徑是在整個家庭網路中引入支援，以便基於每個資料封包的源和目標地址進行路由。雖然大大提高了家庭網路中路由決策的“智慧”，但這種方法需要相對重要的路由器更改，但要避免主機更改。

如前所述，雖然已經提出 NPTv6 用於在網路中提供多宿主支援，但是在家庭網路體系結構中不建議使用它。

應該注意的是，一些多宿主場景可能會看到一個上游是“受防火牆保護的區域”，因此只適合連接到該提供商的服務; 示例可能是 VPN 服務，其僅路由回到家庭網路中的用戶的企業業務網路。根據[RFC3002]的第 4.2.1 節，我們沒有專門針對受防火牆保護的區域多宿主作為本文的目標。

家庭網路體系結構也不應排除使用主機或面向應用的工具，例如 Shim6 [RFC5533]，多路徑 TCP（MPTCP）[RFC6824]或 Happy Eyeballs [RFC6555]。 通常，主機更改獲得的任何增量改進都應該為引入它們的主機帶來好處，但不應該是必需的。

3.2.5. 行動性支援

設備可以在家庭網路內移動。 當駐留在同一子網上時，它們的地址將保持不變，但如果設備移動到不同的（無線）子網，它們將在該子網中獲取新地址。希望家庭網路支援內部設備移動性。 為此，家庭網路可以擴充特定無線子網的範圍以實現跨家庭的無線漫遊（跨家庭的特定子網的可用性）或支援移動性協定以促進使用多個子網的這種漫遊。

3.3. 一個自組織的網路

在與網際網路的連接狀態，設備數量和物理拓撲有關的不同情況下，家庭網路基礎設施應該自然地自組織和自我配置。 同時，高級用戶應該可以手動調整（覆蓋）當前配置。

雖然家庭網路體系結構的目標是使網路盡可能地自組織，但可能存在需要一些手動配置的情況，例如，輸入加密密鑰以應用無線安全性或配置共享路由秘密。 在考慮如何引導路由配置時，後者可能是相關的。 非常希望最小化這種配置的數量。

3.3.1. 區分相鄰的家庭網路

重要的是要避免使用“非預期”設備進行自我配置。 應該有一種方法讓用戶以簡單的方式管理斷言設備是否屬於給定的 homenet。 目標是允許建立邊界，特別是在兩個相鄰的家庭網之間，並避免未經授權的設備參與家庭網路。 這種授權能力可能需要通過家庭網路中的多重跳躍來操作。

因此，家庭網路應該支援家庭網路所有者以合理安全的方式聲明其設備所有權的方式。 這可以通過配對機制來實現，例如，通過在經認證的和新的家庭網路設備上同時按下按鈕或通過作為自主網路環境的一部分的登記過程。

雖然可能存在一個家庭網可能希望故意通過另一個家庭網獲得訪問的情況，例如，共享外部連接成本，但是在本文中沒有討論這種情況。

3.3.2. 最大的實用子網

現在的 IPv4 家庭網路通常只有一個子網，早期的雙堆疊部署只有一個相同的 IPv6 子網，可能還有一些橋接功能。 最近，一些供應商開始引入“家庭”和“訪客”功能，這些功能在 IPv6 中將實現為兩個子網。

由於前面描述的原因，未來的家庭網路極有可能擁有一個或多個內部路由器，因此需要多個子網。 作為網路自組織的一部分，家庭網路應該將自身細分為可以在鏈路層機制，橋接，物理連接和策略以及適用的性能或其他標準的約束下構建的最大實際子網。 在這種細分中，邏輯拓撲可能不一定與物理拓撲匹配。 但是，本文未就如何進行這種細分提出建議。 預計隨後的文件將解決這個問題。

雖然可能希望通過最大化子網的大小來最大化通過家庭網路操作的鏈路本地協定的機會，但是多子網家庭網路是不可避免的，因此必須包括它們的支援。

3.3.3. 處理不同的鏈接技術

家庭網路傾向於多年來有機增長，並且家庭網路通常將建立在來自不同世代的鏈路層技術之上。 目前的家庭網路通常使用從 1 Mbit / s 到 1 Gbit / s 的鏈路 - 吞吐量差異為三個量級。 隨著高速和低功耗技術的部署，我們預計這種差異將進一步擴大。

應該設計家用網路協定以很好地處理非常不同吞吐量的互連鏈路。 特別是，鏈路本地的流不應該在整個家庭網路中氾濫，即使通過多播發送也是如此，並且只要有可能，家庭網協定應該能夠選擇更快的鏈路並避免較慢的鏈路。

鏈路（特別是無線鏈路）也可能具有有限數量的傳輸機會（txops），並且存在明顯的趨勢，其由功率和向下兼容性約束驅動，以將分組聚合到這些有限的 txops 中，同時增加吞吐量。 傳輸機會可能是系統最稀缺的資源，因此也極大地限制了可用的實際吞吐量。

3.3.4. 家庭網路領域和邊界

家庭網路需要了解自己的“站點”的範圍，例如，它將定義 ULA 和站點範圍多播流量的邊界，並且可能需要應用特定的安全策略。家庭網路將與外部連接提供商具有一個或多個此類邊界。

家庭網路很可能也具有內部領域之間的內部邊界，例如客戶領域或公司網路擴充領域。期望可以配置適當的邊界以確定例如可以共享網路前綴，路由訊息，網路流量，服務發現和命名的範圍。內部的默認模式應該是共享所有內容。

預計領域將至少跨越整個子網，因此邊界位於在主網內接收委託前綴的路由器。 對於更豐富的安全模型，還希望主機能夠以與域邊界處的路由器相同的方式基於可用域和相關聯的前綴訊息做出通信決策。

一個簡單的家庭網路模型可能只考慮三種類型的領域和它們之間的邊界，即內部 homenet，ISP 和訪客網路。 在這種情況下，邊界將包括從家庭網到 ISP 的邊界，從訪客網路到 ISP 的邊界，以及從家庭網到訪客網路的邊界。 無論如何，應該可以定義其他類型的領域和邊界，例如，對於某些特定的基於 LLN 的網路，例如智慧電網，並且可以自動檢測這些內容，並應用適當的默認策略來應用哪些類型的流量/數據可以跨越這些邊界。

期望將家庭網路的外部邊界分類為將家庭網路與服務提供商網路分開的唯一邏輯接口。該邊界接口可以是到單個服務提供者的單個物理接口，到單個服務提供者的多個第 2 層子接口，或者到單個或多個提供者的多個連接。此邊界使得可以跨多個功能區域描述邊緣操作和接口要求，包括安全性，路由，服務發現和路由器發現。

家庭網路用戶應該可以覆蓋任何自動確定的邊界以及它們之間應用的默認策略，例外情況是可能無法覆蓋 ISP 在外部邊界定義的策略。

3.3.5. ISP 的組態訊息

在某些情況下，家庭網路從其 ISP 獲取某些配置訊息可能是有用的。 例如，家庭網路 DHCP 服務器可以請求並轉發它從其上游 DHCP 服務器獲得的一些選項，儘管選項的細節可能因部署而異。當然，如果家庭網路是多宿主，那麼這裡有潛在的複雜性。

3.4. 家庭網路定址

家庭網路中使用的 IPv6 定址方案必須符合 IPv6 定址架構 [RFC4291]。在本節中，我們將討論 homenet 如何適應其上游 ISP 提供給它的前綴，以便內部子網，主機和設備可以獲取和配置必要的定址訊息以進行操作。

3.4.1. 使用 ISP 委派的 IPv6 前綴

有關 IPv6 前綴分配策略的討論包含在[RFC6177]中。 實際上，家庭網路可以從其提供者接收任意長度的 IPv6 前綴，例如/ 60，/ 56 或/ 48。 提供的前綴可能是穩定的或不時變化; 通常預計 ISP 將為其住宅用戶提供相對穩定的前綴。 無論如何，家庭網路需要盡可能地適應 ISP 前綴分配策略，並且不假設從 ISP 接收的前綴的穩定性或可能提供的前綴的長度。

但是，例如，如果 ISP 僅提供/ 64，則家庭網路可能受到嚴格限制甚至無法運行。 BCP 157 [RFC6177]聲明如下：

地址管理的一個關鍵原則是，終端站點始終能夠為實際和計劃使用獲得合理數量的地址空間，並且能夠在數年而不是幾個月內指定的時間範圍內。 在實踐中，這意味著至少一個/ 64，並且在大多數情況下顯著更多。必須避免的一個特殊情況是讓終端站點感到被迫使用 IPv6 到 IPv6 網路地址轉換或其他繁瑣的地址保護技術，因為它無法獲得足夠的地址空間。

該體系結構文件假定 ISP 引用了引用文本中的指導。

由於家庭網路沒有為其需求提供足夠的前綴大小，因此會出現許多問題。當面對不足的前綴時，例如使用長於/ 64 的子網前綴（這會破壞無狀態地址自動配置[RFC4862]），而不是試圖設法讓家庭網以受約束的方式運行，使用 NPTv6， 或者回到跨越可能非常不同的媒體的橋接，建議接收路由器改為進入錯誤狀態並發出適當的警告。可能需要考慮如何最好地向典型的家庭用戶呈現這樣的警告或錯誤狀態。

因此，一個家庭網路 CE 路由器應該通過 DHCP 前綴授權（DHCP PD）[RFC3633]請求它想要來自其 ISP 的/ 48 前綴，即它要求 ISP 提供它可能期望的最大大小前綴。 提供，即使在實踐中它可能只提供/ 56 或/ 60。 對於典型的 IPv6 家庭網路，不建議 ISP 提供少於/ 60 的前綴，並且最好 ISP 提供至少 a / 56。預計從任何一個 ISP 分配給家庭網路的前綴是一個連續的，聚合的。雖然家庭網路 CE 路由器可能會發出多個前綴請求以嘗試獲取多個委託，但此類行為超出了本文的範圍。

大型 ISP 的住宅用戶的標準可能類似於他們的單一 IPv4 地址提供;默認情況下，它可能會持續一段時間，但 ISP 自己的配置系統中的更改可能會導致客戶的 IP（以及 IPv6 情況下的前綴池）發生變化。預計 ISP 通常不會支援住宅網路的提供商獨立（PI）定址。

當 ISP 確實需要重組，並且在重新編號其客戶主網時，可能會強制執行“閃存”重新編號。這意味著家庭網路需要能夠處理突然重新編號的事件，與[RFC4192]中描述的過程不同，這將是“旗標日”事件，這意味著優雅的重新編號過程在兩個活動狀態中移動使用前綴是不可能的。雖然重新編號可以被視為初始編號過程的擴充版本，但閃存重新編號和初始“冷啟動”之間的區別在於需要提供服務連續性。

在某些情況下，當地法律意味著某些 ISP 需要為其客戶的隱私原因更改 IPv6 前綴（當前的 IPv4 地址）。在這種情況下，可以避免即時“閃存”重新編號，並根據 RFC 4192 計劃非標記日重新編號。同樣，如果 ISP 有計劃的重新編號過程，則它可能能夠適當地調整租借計時器等。

客戶當然也可以選擇轉移到新的 ISP，從而開始使用新的前綴。在這種情況下，客戶應該期望不連續，並且不僅可以更改前綴，而且如果新 ISP 提供不同的默認大小前綴，則可能還有前綴長度。如果用戶進行了重大的內部“重新管理”，則家庭網路也可能被迫重新編號。

無論如何，家庭網協定支援快速重新編號並且操作過程不會為重新編號過程增加不必要的複雜性。此外，任何新的家庭網路協定的引入都不應該使任何形式的重新編號變得比現在更複雜。

最後，家庭網路的內部操作也應該不依賴於 ISP 網路在任何給定時間的可用性，當然，除了連接到家庭網路外的服務或系統之外。這加強了 ULA 在穩定內部通信中的使用，以及對可在家庭網路中獨立運行的命名和服務發現機制的需求。

3.4.2. 穩定的內部 IP 地址

默認情況下，網路應嘗試在主網的所有內部部分之間以及與外部網際網路之間提供 IP 層連接，但需遵守安全部分中稍後討論的過濾策略或其他策略約束。

無論是否有全球唯一的 ISP 提供的前綴，ULA 都應該在家庭網路的範圍內使用，以支援子網和主機之間的穩定路由和連接。 在長時間外部連接中斷的情況下，ULA 允許跨路由子網的內部操作繼續。 ULA 地址還允許受約束的設備在 IPv6 地址之間創建永久關係，例如，從牆壁控制器到燈，其中符號主機名將需要額外的非易失性儲存器，並且更新睡眠設備中的全局前綴也可能是有問題的。

如前所述，可以預期 ULA 通常與家庭網路中的一個或多個全局前綴一起使用，使得主機變為具有全局唯一和 ULA 前綴的多址。 ULA 應該用於所有設備，而不僅僅是那些只有內部連接的設備。 然後，默認地址選擇將使 ULA 成為使用在同一家庭網路內生成的 ULA 前綴的設備之間的內部通信的首選。

如果在家庭網路中使用 ULA 前綴但沒有外部 IPv6 連接（因此沒有使用 GUA），則應遵循 RFC 7084 中的建議 ULA-5，L-3 和 L-4 以確保正確操作 特別是在家庭網可能是具有 IPv4 外部連接的雙堆疊的情況下。 [RFC4191]中描述的路由訊息選項的使用提供了一種宣告這種更具體的 ULA 路由的機制。

根據 RFC 7084 要求 S-2 的要求，應通過在家庭網路的邊界過濾來限制使用 ULA。

注意，在一些情況下，可能在同一家庭網路內使用多個/ 48 ULA 前綴，例如，當部署網路時，可能也沒有外部連接。 在使用多個 ULA / 48 的情況下，主機需要知道每個/ 48 對於歸屬網是本地的，例如，通過包括在它們的本地地址選擇策略表中。

3.4.3. 內部前綴授權

如上所述，有各種前綴來源。 從家庭網路的角度來看，應該在邊界 CE 路由器[RFC3633]上接收來自每個 ISP 的單個全局前綴。當多個 CE 路由器存在多個 ISP 前綴池時，預計主網內的路由器將

為它們與之通信的每個 ISP 分配自己的前綴。 如上所述，應該提供 ULA 前綴用於穩定的內部通信或用於受約束/ LLN 網路。

對家庭網路的委託或前綴池的可用性應允許後續內部自主分配前綴以在家庭網路中使用。 這種內部分配不應該採用平面或分層模型，也不應該假設內部前綴的分配是分佈式的還是集中式的。 分配機制應該提供合理的效率，因此典型的家庭網路前綴分配大小在大多數情況下可以容納所有必要的/ 64 分配，而不是浪費前綴。 此外，應該避免將多個/ 64 個重複分配到同一網路，並且在前綴耗盡的情況下網路應該盡可能優雅地行為（儘管在這種情況下的選項可能是有限的）。

在家庭網路具有多個 CE 路由器並且這些是來自其連接的 ISP 的委託前綴池的情況下，預期內部前綴分配將由每個 CE 路由器為與其相關聯的每個前綴提供服務。 在使用 ULA 的情況下，最好只有一個/ 48 ULA 覆蓋整個家庭網路，從中可以分配 64 個子網。 如果在家庭網路中生成兩個/ 48 個 ULA，網路仍應繼續運行，這意味著主機需要確定每個 ULA 是本地網路的本地。

家庭網路中的前綴分配應該為每個鏈路分配一個穩定的前綴，該前綴在重新啟動，斷電和類似的短期中斷時保持不變。 持久性前綴的可用性不應取決於路由器引導順序。 添加新的路由設備不應該影響現有的持久性前綴，但面對家庭網路的重大“重新管理”，可能不會出現持久性。 但是，在家庭網路中分配的 ULA 前綴應該通過 ISP 驅動的重新編號事件保持持久性。

提供這樣的持久性前綴可能意味著需要在路由設備上進行穩定儲存，並且還需要一種家庭用戶“重置”所儲存的前綴的方法，如果需要進行重大的重新配置（儘管理想情況下，家庭用戶根本不應該參與）。

本文沒有針對解決方案提出具體建議，但指出參與家庭網路的所有路由設備很可能必須使用相同的內部前綴委派方法。 這意味著只應使用一種委託方法。

3.4.4. 配置訊息的協調

網路元件將需要以考慮在不同元件上使用的定時器上的各種壽命的方式集成，例如，DHCPv6 PD，路由器，有效前綴和優選前綴定時器。

3.4.5. 隱私

如果 ISP 向客戶提供相對穩定的 IPv6 前綴，則與家庭網路相關聯的地址的網路前綴部分可能不會在相當長的時間段內發生變化。

因此，來自同一家庭網路的流量的暴露類似於 IPv4; 通過使用 IPv4 NAT 看到的單個 IPv4 全局地址提供與 IPv6 流量所見的全局 IPv6 前綴相同的提示。

雖然 IPv4 NAT 可能會混淆內部設備流量來自的外部觀察者，但即使使用隱私地址[RFC4941]，IPv6 也會增加額外的曝光，即通過使用相同的 IPv6 源地址從同一內部設備獲取流量 一段時間。

3.5. 路由功能性

當內部家庭網路中部署了多個路由器時，需要路由功能。此功能可以像 IPv4 NAT 的當前“默認路由已啟動”模型一樣簡單，或者更可能的是，它將涉及運行適當的路由協定。

需要一種機制來發現家庭網路中的哪個（哪些）路由器提供 CE 路由器功能。邊界可以包括但不限於到上游 ISP 的接口，到諸如 LLN 網路的單獨家庭網路的閘道器設備，或到訪客或私人公司擴充網路的閘道器。在某些情況下，可能沒有邊界存在，例如，可能在建立上游連接之前發生。

如前所述，路由環境應該是自配置的。家庭網路自配置過程和路由協定必須以可預測的方式進行交互，尤其是在啟動和重新收斂期間。邊界發現功能和其他自配置功能可以集成到路由協定本身中，但也可以通過單獨的發現機制導入。

理想狀況是通過單獨的配置協定在家庭網路內散佈和同步配置訊息。

家庭網路路由協定應基於先前部署的協定，該協定已被證明是可靠且健壯的。這並不排除選擇可以獲得高質量開源實現的新協定。生成的代碼必須支援輕量級實現，並且適合結合到消費設備中，其中固定和臨時儲存和處理能力都非常寶貴。

在給定的家庭網路中，在給定時間最多應使用一個單播和一個多播路由協定。 在一些簡單的拓撲中，可能不需要路由協定。 如果給定家庭網路中的路由器支援多個路由協定，則需要一種機制來確保該家庭網路中的所有路由器使用相同的協定。

家庭網路體系結構僅限 IPv6。 實際上，如第 3.2.3 節所述，在可預見的未來，雙堆疊家庭網路仍有可能出現。 雖然對 IPv4 和其他地址族的支援可能因此是有益的，但並不明確要求在相同的路由協定中攜帶路由訊息。

在家庭網路路由拓撲中必須考慮多種類型的物理接口。諸如乙太網路，Wi-Fi，同軸電纜多媒體聯盟（MoCA）等技術必須能夠在相同的環境中共存，並且應當被視為任何路由部署的一部分。應考慮在路徑計算中包含物理層特性以優化家庭網路中的通信。

3.5.1. 家庭網路中的單播路由

單播路由協定的作用是提供足夠好的端到端連接，足夠好/經常足夠由用戶期望定義。

由於使用各種不同的底層鏈路技術，家庭網路中的路徑選擇可能比最小化跳數更精確。對於流量來說，在可用的主網路內使用到達給定目的地的多個路徑而不僅僅是單個最佳路徑也可能是有益的。

最小化收斂時間應該是任何路由環境中的目標。可以合理地假設收斂時間不應該明顯長於用戶在 CE 路由器重啟時習慣的網路中斷。

家庭網路體系結構與底層路由技術的選擇無關，例如鍊路狀態與 Bellman-Ford。

路由協定應支援多個客戶網際網路連接的通用使用以及多個委派前綴的並發使用。因此，非常需要能夠根據源地址和目標地址做出路由決策的路由協定，以避免 BCP 38 中描述的上游 ISP 入口過濾問題。多宿主支援還可以包括對多個提供商的負載平衡以及從主服務器到主服務器的故障轉移備份鏈接可用時。該協定不應要求建立上游 ISP 連接以繼續在家庭網路內路由。

家庭網路體系結構與路由協定必須支援的最小跳數無關。但是，該體系結構應該可以擴充到可以部署家庭網路技術的其他場景，其中可能包括小型辦公室和小型企業站點。為了允許這樣的情況，期望該架構可擴充到更高的跳數和更大數量的路由器，而不是真正的家庭網路中的典型。

在撰寫本文時，隨著網路開始採用傳統乙太網路技術和為 LLN 設計的鏈路層（例如用於某些類型的傳感器設備的鏈路層），鏈路層網路技術將變得更加異構。

理想情況下，LLN 或其他邏輯上獨立的網路應該能夠交換路由，以便 IP 流量可以通過與主網和任何 LLN 互操作的閘道器路由器在網路之間轉發。當前的家庭部署在傳感器和基本網際網路連接網路中使用很多不同的機制。IPv6 虛擬機（VM）解決方案還可能添加其他路由要求。

在這種家庭網路體系結構中，LLN 和其他專用網路被認為是家庭網路的存根區域，因此不希望它們在更傳統的媒體之間充當流量傳輸。

3.5.2. 家庭網路邊界的單播路由

[RFC7084]中定義的當前實踐表明，家庭網路 CE 路由器和服務提供商路由器之間的路由遵循[RFC7084]第 4 節（WAN 端要求）中的 WAN 端要求模型，至少在初始部署中如此。但是，考慮在家庭網路 CE 路由器和服務提供商路由器之間是否使用路由協定超出了本文的範圍。

3.5.3. 多播支援

期望的是，根據某些媒體類型上的設備的容量，跨越家庭網路支援多播路由，包括特定來源群播（SSM）[RFC4607]。

[RFC4291]要求在管理上配置範圍 4 或更高的任何邊界（即，admin-local 或更高）。 因此，必須在管理上配置家庭網路-ISP 邊界的邊界，儘管這可能由諸如 DHCP PD 之類的管理功能觸發。其他多播轉發策略邊界也可以存在於家庭網路內，例如，到/來自訪客子網，而某些鏈路媒體類型的使用也可以影響特定多播流量被轉發或路由的位置。

在家庭網路上支援多播可能有不同的驅動程序 -- 例如，

- 對於家庭網路服務發現，應該定義範圍大於鏈路本地的多播服務發現協定

- 用於基於多播的流式傳輸或文件共享應用程序

在通過家庭網路路由多播的情況下，需要適當的多播路由協定，根據單播路由協定應該是自配置的。 如上所述，必須能夠對多播流量進行範圍調整或過濾，以避免它被泛洪到設備無法合理支援的網路媒體。

家庭網路不僅可以在內部使用多播，它還可以是外部多播流量的消費者或提供者，其中家庭網路的 ISP 支援這種多播操作。例如，這可能是有價值的，其中直播視頻應用程序來自/來自家庭網路。

多播環境應支援應用程序選擇要使用的唯一多播組的能力。

3.6. 安全

IPv6 家庭網路的安全性是一個重要的考慮因素。 與 IPv4 營運模式最顯著的區別在於 NAT 的移除，設備的全局可定址性的引入，因此需要考慮設備是否應具有全局可達性。 無論如何，主機需要能夠安全地運行，在需要時端到端運行，並且還能夠抵禦針對它

們的惡意流量。 然而，引入了其他挑戰，例如，各種家庭網域之間的邊界處的默認過濾策略。

3.6.1. 定址能力與可達性

基於 IPv6 的家庭網路架構應該採用透明的端到端通信模型，如[RFC2775]中所述。 每個設備應該是全球可定址的，並且這些地址在傳輸過程中不得更改。但是，可以應用安全邊界來限制端到端通信，因此雖然主機可以是全局可定址的，但它可能不是全局可達的。

[RFC4864]描述了用於 IPv6 網路的“簡單安全”模型，其中可以應用有狀態周邊過濾來控製家庭網路中設備的可達性。RFC 4864 在 4.2 節中指出“除了主機防御之外，還建議那些需要邊界保護的人使用防火牆.....”應當注意，“默認拒絕”過濾方法將有效地取代對 IPv4 NAT 遍歷協定的需要，需要使用信號協定來請求打開防火牆，例如，諸如 PCP [RFC6887]之類的協定。 在具有多個 CE 路由器的網路中，信號將需要處理可能使用一個或多個出口路由器的流的情況。 CE 路由器需要能夠為這些協定通告它們的存在。

[RFC6092]擴充了 RFC 4864，更詳細地討論了 IPv6 邊界安全建議，而沒有強制要求採用“默認拒絕”方法。實際上，RFC 6092 並未強制執行特定的操作模式，而是聲明 CE 路由器必須提供允許“透明”模式的易於選擇的配置選項，從而確保“默認允許”模型可用。

關於本文中描述的未來家庭網路是否應具有“默認拒絕”或“默認允許”位置的主題已在各種 IETF 會議中詳細討論，未就哪種方法更合適達成共識。 此外，應用哪個默認值可能是情境性的，因此本文不會對 RFC 6092 中關於此主題所寫內容的默認設置提出建議。我們在下面的第 3.6.3 節中註意到隱式防火牆功能。IPv4 NAT 在今天很常見，因此針對家庭網路的未來 CE 路由器應該繼續支援以“默認拒絕模式”運行的選項，無論這是否是默認設置。

3.6.2. 邊界過濾

如前所述，期望存在檢測主網內不同類型邊界的機制，以及然後在這些邊界應用不同類型的過濾策略的其他機制，例如，命名和服務發現是否應該通過給定邊界。任何這樣的策略應該能夠由典型的家庭用戶容易地應用，例如，以使訪客網路中的用戶訪問家庭中的媒體服務或訪問打印機。將需要簡單的機制來應用策略更改或設備之間的關聯。

在某些情況下，例如在某些公用事業網路場景中，可能不需要完全的內部連接，或者出於策略原因需要對來賓網路子網進行過濾。結果，某些方案/模型可能涉及使用其自己的 CE 路由器運行隔離的子網。在這種情況下，只能在每個隔離的網路內實現連接性（儘管流量可能會通過外部提供商在它們之間傳遞）。

LLN 提供了另一個在 homenet 內可能存在安全邊界的示例。受約束的 LLN 節點可以實現網路密鑰安全性，但可能依賴於 LLN 邊界路由器強制執行的訪問策略。

第 3.3.1 節討論了區分相鄰主網的注意事項。

3.6.3. NAT 和防火牆的部分有效

通過朦朧保全（地址轉換）或通過防火牆（過濾）的安全性充其量只是部分有效。 家用電腦，家庭網路，商用 PC 電腦和網路的安全記錄非常糟糕，這證明了這一點。任何設備的防火牆背後的安全妥協都會暴露所有其他設備，使整個網路依賴於隱匿性或防火牆，因為它是網路私有端最不安全的設備。

但是，鑑於目前有關家庭網路產品的默認設備安全性非常差的證據，將防火牆置於適當位置確實提供了一定程度的保護。今天使用防火牆，無論是否良好實踐，都是常見的做法，並且不應該丟失通過“默認拒絕”設置提供保護的能力，即使是有效的。因此，雖然非常希望家庭網路中的所有主機都能通過內置安全功能得到充分保護，但也應該假設所有 CE 路由器將繼續支援適當的外圍防禦功能，如[RFC7084]所述。

3.6.4. 滲透問題

隨著家庭網路變得越來越複雜，設備越來越多，並且可能在整個家庭中啟用服務發現，如果設備使用發現協定來收集訊息並將其報告給設備供應商或應用服務提供商，則可能會對訊息洩漏產生擔憂。

雖然不清楚如何輕易避免這種滲透，但應該認識到威脅，無論是來自新的硬體還是安裝在個人設備上的某些應用程式。

3.6.5. 設備功能

在設備方面，homenet 主機應根據其計算能力實施自己的安全策略。
對於所有端口或特定服務，它們應具有請求透明通信的方法，該透明通信可通過本地網中的安全篩選器啟動給它們。用戶應該有簡單的方法將設備與希望通過（CE 路由器）邊界透明地運行的服務相關聯。

3.6.6. ULA 作為連接起點的指示

如第 3.6 節所述，如果在 CE 路由器上有適當的過濾，如 RFC 7084 中的要求 S-2 所規定的那樣，ULA 源地址可以作為本地源流量的指示。 如果 ULA 地址空間在領域的邊界被適當地過濾，則該指示可以與安全設置一起用於指定允許特定應用程序在哪些節點之間通信。

3.7. 命名和服務發現

家庭網路要求設備能夠確定和使用唯一的名稱，通過這些名稱可以在網路上訪問它們，並且網路上的其他設備不會使用這些名稱。用戶和設備將需要能夠發現網路上可用的設備和服務，例如媒體服務器，打印機，顯示器或特定的家庭自動化設備。 因此，必須在家庭網路中支援命名和服務發現，並且考慮到典型家庭網路用戶的性質，提供此功能的服務必須盡可能支援非管理操作。

無論用戶是在主網內還是在主網之外，命名系統都需要在內部或外部工作，即，用戶應該能夠通過名稱引用設備，並且無論它們

在哪裡，都可能連接到它們。考慮這種命名和服務發現的最自然的方式是使其能夠在整個家庭網路住宅（站點）上工作，忽略諸如子網之類的技術邊界，但尊重諸如客戶和其他內部網路領域之間的政策邊界。家庭網路居民在旅行時可能需要遠程訪問，但也可能是製造商或其他“仁慈”的第三方。

3.7.1. 發現服務

用戶通常將通過圖形用戶界面（GUI）執行服務發現，這些界面允許他們以適當且直觀的方式瀏覽其網路上的服務。設備可能還需要發現其他設備，無需任何用戶干預或選擇。無論哪種方式，此類接口都超出了本文的範圍，但接口應具有適當的應用程序編程接口（API），以便執行發現。

此類接口通常還可以隱藏用戶的本地域名元素，尤其是在只有一個名稱空間可用的情況下。但是，正如我們在下面討論的那樣，在某些情況下，發現可用域的能力可能很有用。

我們注意到，當前的零配置服務發現協定通常針對單個子網。因此，可以選擇使多子網歸屬網來確定是應該代理還是擴充這些協定以在整個家庭網路上運行。在這種情況下，這可能意味著橋接本地鏈路方法，注意避免資料封包進入循環路徑，或擴充用於此目的的多播流量範圍。這可能意味著使用了一些代理或混合服務，可能共同駐留在 CE 路由器上。或者，可能新方法是優選的，例如，將家庭網路周圍的訊息作為路由協定內的屬性（其可以允許每個前綴配置）泛洪。但是，我們應該更喜歡向後兼容的方法，並允許繼續使用當前的實現。請注意，本文並未強制要求特定的解決方案;相反，它表達了應該用於家庭網路命名和服務發現環境的原則。

當今服務發現面臨的主要挑戰之一是由於可用的服務發現協定數量不斷增加而缺乏互操作性。雖然可以想像消費者設備支援多種發現協定，但這顯然不是網路和計算資源的最有效使用。家庭網路體系結構的一個目標應該是通過基於標準的轉換方案，掛鉤到當前協定以允許發現協定之間的某種形式的通信，支援家庭網路中的中央服務儲存庫的擴充，或者服務發現協定互操作性的路徑，或者 簡單地向統一的協定套件收斂。

3.7.2. 指定名稱給設備

鑑於將來可以聯網的大量設備，設備應該具有在家庭網路中生成它們自己的唯一名稱並且在它們出現時檢測衝突的手段，例如，相同類型/供應商的第二設備作為 部署具有相同默認名稱的現有設備，或者將新子網添加到已具有相同名稱的設備的家庭網路中。在主網的範圍內，設備應該具有固定的名稱。

用戶也將希望使用簡單的方法（重命名）設備，同樣很可能是通過本文範圍之外的適當且直觀的界面進行的。請注意，用戶分配給設備的名稱可能是作為設備屬性儲存在設備上的標籤，並且可能與名稱服務中使用的名稱不同，例如，“Study Laser Printer”對應到 printer2.<somedomain>。

3.7.3. 家庭網路名稱服務

家庭網路名稱服務應支援查找和發現。查找將通過對已知服務的直接查詢來操作，而發現可以使用多播消息或應用程序註冊以便找到的服務。

非常希望家庭網路名稱服務必須至少與因特網名稱服務共存。對現有的成熟解決方案也應該有偏見。因此，強烈的暗示是家庭網服務是基於 DNS 或 DNS 兼容的。有一些命名協定可以在網際網路上進行配置和操作，如基於單播的 DNS，還有為零配置本地環境設計的協定，如多播 DNS（mDNS）[RFC6762]。

當 DNS 用作家庭網路名稱服務時，它通常包括解析服務和權威服務。 權威服務託管與家庭網路相關的區域。 提供這樣的名稱服務（一種旨在促進全球網際網路名稱解析）的一種方法是在 CE 路由器上運行權威名稱服務，以及由 ISP 或外部第三方提供的輔助權威名稱服務。

在使用零配置名稱服務的情況下，希望它們也可以與因特網名稱服務共存。特別地，在家庭網路使用全局名稱空間的情況下，期望設備具有在需要時向該名稱空間添加條目的能力。還應該有一種機制可以從全局名稱空間中刪除或終止此類條目。

為了防止緩存中毒等攻擊，攻擊者能夠在本地緩存中插入偽造的 DNS 條目，需要在兩者上支援適當的名稱服務安全方法，包括 DNS 安全擴充（DNSSEC）[RFC4033]。 權威服務器和解析器方面。 在使用 DNS 的情況下，homenet 路由器或命名服務不得阻止 DNSSEC 運行。

雖然本文未指定硬體要求，但值得注意的是，例如，為了支援 DNSSEC，適當的家庭網設備應具有良好的隨機數生成能力，未來的家庭網規範應指明高質量隨機數生成器的位置，即 需要具有良好的熵。

最後，必須考慮 CE 路由器變化的影響。 期望保留舊 CE 路由器中保持的任何相關狀態（配置）。 這可能意味著狀態訊息應該在家庭網路中散佈，可以由新的 CE 路由器恢復，或者通過某種方式恢復到家庭網路的 ISP 或第三方外部提供的服務。

3.7.4. 名稱空間

如果需要從網際網路上的任何位置遠程訪問家庭網路設備，則至少需要一個全局唯一的名稱空間，但不應排除使用多個名稱空間。一種方法是用於家庭網路的名稱空間將由家庭網路權威地提供，很可能由駐留在 CE 路由器上的服務器提供。 這些名稱空間可以由用戶獲取，或者由其 ISP 或外部提供的替代服務提供/生成。默認情況下，家庭網路將使用 ISP 提供的全局域，但是希望長期使用獨立於其提供者的名稱空間的高級用戶應該能夠獲取和使用他們自己的域 名稱。 對於想要使用自己的獨立域名的用戶，此類服務已經可用。

還可以在不同的名稱空間中為設備分配不同的名稱，例如，可以代表居民管理家庭網路中的系統或設備的第三方。家庭網路的遠程管理超出了本文的範圍。

但是，如果全局名稱空間不可用，則主機網將需要選擇並使用本地名稱空間，該空間僅在本地主網中具有意義（即，它不會用於遠程訪問主網）。 .local 名稱空間當前對於具有鏈接本地範圍的

某些現有協定具有特殊含義，因此不適用於多子網家庭網路。 因此，家庭網路需要不同的名稱空間。

選擇本地名稱空間的一種方法是使用不明確的本地限定域名（ALQDN）空間，例如.sitelocal（或為此目的保留的適當名稱）。 雖然這是一種簡單的方法，但原則上有可能通過一個家庭網路中的應用程序按名稱以某種方式加入書籤的設備與另一個家庭網路中具有相同名稱的設備混淆。 然而，在實踐中，底層服務發現協定應該能夠處理移動到網路，其中新設備使用與先前在另一家庭網路中使用的設備相同的名稱。

本地名稱空間的另一種方法是使用唯一的本地限定域名（ULQDN）空間，例如 .<UniqueString>.sitelocal。<UniqueString>可以以多種方式生成，一種可能基於在主網上使用的本地/ 48 ULA 前綴。 這樣的<UniqueString>應該在冷啟動後繼續存在，即在網路斷電後保持一致，或者如果在啟動時沒有設置值，則 CE 路由器或運行名稱服務的設備應該生成默認值。希望家庭網路用戶能夠用他們選擇的值覆蓋<UniqueString>，但這會增加名稱衝突的可能性。任何生成的<UniqueString>都不應該是可預測的; 因此，需要添加 salt / hash 函數。

在（可能）事件中，可以從家庭網路外部訪問家庭網路（使用全局名稱空間），因此家庭網路名稱空間遵循全局名稱空間的規則和約定至關重要。 在此操作模式下，家庭網路中的名稱（包括由設備自動生成的名稱）必須可用作全局名稱空間中的標籤。 [RFC5890]描述了在應用程序中國際化域名（IDNA）的注意事項。

此外，隨著新的“無點”頂級域名的引入，例如，稱為“計算機”的本地主機和（如果已註冊）計算機通用頂級域名（gTLD）之間也存在模糊性的可能性。。 因此，應始終使用限定名稱，無論這些名稱是否暴露給用戶。 IAB 發表了一份聲明，解釋了為什麼無網域應被視為有害[IABdotless]。

可能存在這樣的用例：對於家庭網路中的不同領域或者家庭網路內的單個名稱空間的分段，可能需要不同的名稱空間。 因此，可

能需要分層名稱空間管理。還應該沒有什麼可以防止單個設備在外部名稱空間中獨立註冊。

可能的情況是，如果有兩個或更多 CE 路由器為家庭網路服務，如果每個路由器具有從不同 ISP 委派的名稱空間，則家庭中的設備有可能在多個域下具有多個完全限定名稱。

在用戶處於希望訪問其歸屬網路中的設備的遠程網路中的情況下，可能需要考慮所呈現的域搜索順序，其中存在多個相關聯的名稱空間。 這也意味著需要域發現功能。

可能的情況是，並非通過網際網路名稱空間通過名稱可以使用歸屬網路中的所有設備，並且某些設備更喜歡使用“拆分視圖”（如[RFC6950]第 4 節中所述）。 家庭網路看到的 DNS 回應與外部的回應不同。

最後，本文沒有假設反向查找服務的存在或遺漏。有一種觀點認為，向具有有意義的設備名稱而不是文字地址的用戶顯示日誌記錄訊息可能很有用。還有一些服務,尤其是電子郵件郵件交換器，其中一些營運商在接受連接之前選擇要求有效的反向查找。

3.7.5. 獨立運作

如果本地網路與全球網際網路斷開連接，則可到達設備的名稱解析和服務發現必須繼續起作用，例如，即使網際網路鏈路長時間停機，本地媒體服務器仍應可用。這意味著本地網路還應該能夠在沒有外部連接的情況下執行完全重啟，並使本地命名和服務發現正常運行。

如上所述，具有高速緩存的本地權威名稱服務的方法將允許本地操作以用於持續的 ISP 中斷。

如果外部連接不可用，則需要具有獨立的本地信任鏈以支援安全交換。

ISP 的更改不應影響本地命名和服務發現。 但是，如果家庭網路使用 ISP提供的全局名稱空間，那麼如果用戶更改其網路提供商，這顯然會產生影響。

3.7.6. LLNs 的考慮因素

在家庭網路的一些部分中，特別是 LLN 或使用電池電源的任何設備，設備可能正在休眠，在這種情況下，可能需要可以響應（例如）多播服務發現請求的這種節點的代理。 那些相同的設備或網路的部分可能具有較少的可能從網路的其他部分泛洪的多播流量的容量。 通常考慮到服務可能需要操作的網路技術和受限制設備，消息利用應該是有效的。

正在確定由 LLN 網路中的約束應用協定（CoAP）[RFC7252]使用的命名和發現解決方案。 這些超出了本文的範圍。

3.7.7. DNS 解析器探索

需要自動發現名稱服務以允許家庭網路中的客戶端設備解析網際網路上的外部域，並且此類發現必須支援可能遠離名稱服務的多個路由器躍點的客戶端。 類似地，可能希望傳達可能對家庭網路有效的任何 DNS 域搜索列表。

3.7.8. 漫游到家庭網路的設備

一些在家庭網路網際網路名稱空間內註冊名稱且行動設備的設備可能會在其他位置連接到網際網路並在這些位置獲取 IP 地址。 設備可以在不同的主網之間移動。 在這種情況下，希望可以通過與其歸屬網路中使用的名稱相同的名稱來訪問設備。

本文不討論此問題的解決方案。 它們可能包括使用行動 IPv6 或動態 DNS（其中任何一個都會對家庭網路提出額外要求）或建立到家庭網路中服務器的（VPN）隧道。

3.8. 其他考慮因素

本節討論了家庭網路的另外兩個注意事項，架構不應該排除，但這個文本是中性的。

3.8.1. 服務質量

在多服務家庭網路中支援服務質量（QoS）可能是一項要求，例如，對於關鍵系統（可能與醫療保健相關）或在不同類型的流量之間進行區分（文件共享，雲儲存，直播，語音）通過 IP（VoIP）等）。 不同的鏈接媒體類型可以具有不同的這種屬性或能力。

但是，家庭網路方案應該不需要新的 QoS 協定。 具有少量預定義流量類的 Diffserv [RFC2475]方法通常就足夠了，儘管目前在家庭網路中幾乎沒有 QoS 部署的經驗。CE 路由器可能需要 QoS 或流量優先級方法，並且可能在不同鏈路媒體類型之間的邊界（例如，某些流量可能根本不適合某些媒體，需要丟棄以避免超載受約束的媒體）。

也可能存在可能有益於家庭網域中的應用程序性能和行為的補充機制，例如確保使用[Gettys11]中描述的適當緩衝算法。

3.8.2. 運作和管理

在本節中，我們將簡要回顧一下本文中描述的家庭網路類型的操作和管理的一些初始注意事項。預計單獨的文件將為這些家庭網路定義適當的操作和管理框架。

如本文中所述，家庭網路的總體目標應該是從網路層角度進行自組織和自我配置，例如，前綴應該能夠分配給路由器接口。此外，在設備上運行的應用程序應該能夠使用零配置服務發現協定來發現家庭用戶感興趣的服務。 相反，例如，不期望家庭用戶必須為鏈接分配前綴或管理家庭網路的 DNS 條目。 不應排除這種專家操作，但這不是常態。

用戶可能仍然需要或希望執行網路及其上的設備的某些配置。示例可能包括輸入安全密鑰以啟用對其無線網路的訪問，或選擇為通過服務發現呈現給他們的設備提供“親和名稱”。鏈接層和應

用層服務的配置超出了本架構原則文件的範圍，但可能在營運的家庭網路中需要。

雖然不期望主動配置其家庭網路的網路元素，但用戶可能對能夠查看其網路狀態及與其連接的設備感興趣，在這種情況下，將需要適當的網路監視協定以允許他們查看 他們的網路及其狀態，例如，通過網路界面或等同物。雖然用戶可能不了解網路的運行方式，但可以合理地假設他們有興趣了解網路上可能存在哪些故障或問題。這種監視可以擴充到網路上的其他設備，例如儲存設備或網路攝像機，但是這樣的設備超出了本文的範圍。

也可能是 ISP 或第三方可能希望代表用戶為家庭網路提供遠程管理服務，或者能夠在他們遇到某些問題時協助用戶，在這種情況下，需要適當的管理和監測協定。

指定促進家庭網路管理和監控所需的協定超出了本文的範圍。如上所述，預計將編制一份單獨的文件來描述本文件中提出的各類家庭網路的運作和管理框架。

最後，我們注意到所有網路管理和監控功能都應該通過 IPv6 傳輸提供，即使在家庭網是雙堆疊的情況下也是如此。

3.9. 在 IPv6 上實現架構

該體系結構文本鼓勵重用現有協定。因此，必要的機制在很大程度上已經是 IPv6 協定集和通用實現的一部分，儘管有一些例外。

對於自動路由，期望可以基於現有協定找到解決方案。可能需要一些相對較小的更新，例如，可能需要新機制以便默認啟用所選協定，或者可能需要一種機制來自動為主網內的鏈路分配前綴。

如果架構需要，某些功能可能需要更大的改變或需要開發新協定，例如，支援多宿主路由器的多宿主可能需要擴充以支援家庭網路內的基於源和目的地址的路由。

但是，體系結構中需要進行一些協定更改，例如，為了進行名稱解析和服務發現，需要擴充現有的零配置鏈接本地名稱解析協定，以使其能夠在家庭網路範圍內跨子網工作。

開發家庭網路 IPv6 架構解決方案中的一些最難的問題包括發現“主頁”域結束且服務提供商域開始的正確邊界，確定某些必要的發現機制擴充是否應僅影響網路基礎架構或主機，以及以向後兼容的方式打開路由，前綴委派和其他功能的能力。

4. 結論

本文定義了家庭網路體系結構的原則和要求。此處記錄的原則和要求應該通過描述用於路由，前綴管理，安全性，命名或服務發現的家庭網路協定的任何未來文本來觀察。

5. 安全考慮因素

以上第 3.6 節討論了家庭網路體系結構的安全注意事項。

6. 參考資料

6.1. 正規參考文獻

[RFC2460] Deering, S. and R. Hinden, "網際網路 Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998, <http://www.rfc-editor.org/info/rfc2460>.

[RFC3633] Troan, O. and R. Droms, "IPv6 Prefix Options for Dynamic Host Configuration Protocol (DHCP) version 6", RFC 3633, December 2003, <http://www.rfc-editor.org/info/rfc3633>.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005, <http://www.rfc-editor.org/info/rfc4193>.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6

Addressing Architecture", RFC 4291, February 2006,
<http://www.rfc-editor.org/info/rfc4291>.

6.2. 資訊參考

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and
E. Lear, "Address Allocation for Private 網際網路s", BCP 5, RFC 1918, February 1996,
<http://www.rfc-editor.org/info/rfc1918>.

[RFC2475] Blake, S., Black, D., Carlson, M., Davies, E., Wang, Z., and W. Weiss, "An Architecture for Differentiated Services", RFC 2475, December 1998,
<http://www.rfc-editor.org/info/rfc2475>.

[RFC2775] Carpenter, B., "網際網路 Transparency", RFC 2775, February 2000,
<http://www.rfc-editor.org/info/rfc2775>.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000,
<http://www.rfc-editor.org/info/rfc2827>.

[RFC3002] Mitzel, D., "Overview of 2000 IAB Wireless 網際網路working Workshop", RFC 3002, December 2000,
<http://www.rfc-editor.org/info/rfc3002>.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001,
<http://www.rfc-editor.org/info/rfc3022>.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and

Requirements", RFC 4033, March 2005, <http://www.rfc-editor.org/info/rfc4033>.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, November 2005, <http://www.rfc-editor.org/info/rfc4191>.

[RFC4192] Baker, F., Lear, E., and R. Droms, "Procedures for Renumbering an IPv6 Network without a Flag Day", RFC 4192, September 2005, <http://www.rfc-editor.org/info/rfc4192>.

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, August 2006, <http://www.rfc-editor.org/info/rfc4607>.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007, <http://www.rfc-editor.org/info/rfc4862>.

[RFC4864] Van de Velde, G., Hain, T., Droms, R., Carpenter, B., and E. Klein, "Local Network Protection for IPv6", RFC 4864, May 2007, <http://www.rfc-editor.org/info/rfc4864>.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007, <http://www.rfc-editor.org/info/rfc4941>.

[RFC5533] Nordmark, E. and M. Bagnulo, "Shim6: Level 3 Multihoming Shim Protocol for IPv6", RFC 5533, June 2009, <http://www.rfc-editor.org/info/rfc5533>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, August

2010,
<http://www.rfc-editor.org/info/rfc5890>.

[RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010,
<http://www.rfc-editor.org/info/rfc5969>.

[RFC6092] Woodyatt, J., "Recommended Simple Security Capabilities in Customer Premises Equipment (CPE) for Providing Residential IPv6 網際網路 Service", RFC 6092, January 2011,
<http://www.rfc-editor.org/info/rfc6092>.

[RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, April 2011,
<http://www.rfc-editor.org/info/rfc6144>.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011,
<http://www.rfc-editor.org/info/rfc6145>.

[RFC6177] Narten, T., Huston, G., and L. Roberts, "IPv6 Address Assignment to End Sites", BCP 157, RFC 6177, March 2011,
<http://www.rfc-editor.org/info/rfc6177>.

[RFC6204] Singh, H., Beebee, W., Donley, C., Stark, B., and O. Troan, "Basic Requirements for IPv6 Customer Edge Routers", RFC 6204, April 2011,
<http://www.rfc-editor.org/info/rfc6204>.

[RFC6296] Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix Translation", RFC 6296, June 2011,
<http://www.rfc-editor.org/info/rfc6296>.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual- Stack Lite Broadband Deployments

Following IPv4 Exhaustion", RFC 6333, August 2011, <http://www.rfc-editor.org/info/rfc6333>.

[RFC6555] Wing, D. and A. Yourtchenko, "Happy Eyeballs: Success with Dual-Stack Hosts", RFC 6555, April 2012, <http://www.rfc-editor.org/info/rfc6555>.

[RFC6724] Thaler, D., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for 網際網路 Protocol Version 6 (IPv6)", RFC 6724, September 2012, <http://www.rfc-editor.org/info/rfc6724>.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, February 2013, <http://www.rfc-editor.org/info/rfc6762>.

[RFC6824] Ford, A., Raiciu, C., Handley, M., and O. Bonaventure, "TCP Extensions for Multipath Operation with Multiple Addresses", RFC 6824, January 2013, <http://www.rfc-editor.org/info/rfc6824>.

[RFC6887] Wing, D., Cheshire, S., Boucadair, M., Penno, R., and P. Selkirk, "Port Control Protocol (PCP)", RFC 6887, April 2013, <http://www.rfc-editor.org/info/rfc6887>.

[RFC6950] Peterson, J., Kolkman, O., Tschofenig, H., and B. Aboba, "Architectural Considerations on Application Features in the DNS", RFC 6950, October 2013, <http://www.rfc-editor.org/info/rfc6950>.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, November 2013, <http://www.rfc-editor.org/info/rfc7084>.

[RFC7157] Troan, O., Miles, D., Matsushima, S., Okimoto, T., and D. Wing, "IPv6 Multihoming without Network Address Translation", RFC 7157, March 2014, <http://www.rfc-editor.org/info/rfc7157>.

[RFC7252] Shelby, Z., Hartke, K., and C. Bormann, "The Constrained Application Protocol (CoAP)", RFC 7252, June 2014, <http://www.rfc-editor.org/info/rfc7252>.

[IABdotless]
IAB, "IAB Statement: Dotless Domains Considered Harmful", February 2013, <http://www.iab.org/documents/correspondence-reports-documents/2013-2/iab-statement-dotless-domains-considered-harmful>.

[Gettys11]
Gettys, J., "Bufferbloat: Dark Buffers in the 網際網路", March 2011, <http://www.ietf.org/proceedings/80/slides/tsvarea-1.pdf>.

致謝

作者要感謝 Mikael Abrahamsson，Aamer Akhter，Mark Andrews，Dmitry Anipko，Ran Atkinson，Fred Baker，Ray Bellis，Teco Boot，John Brzozowski，Cameron Byrne，Brian Carpenter，Stuart Cheshire，Julius Chroboczek，Lorenzo Colitti，Robert Cragie ，艾爾文·戴維斯（Elwyn Davies），拉爾夫·德羅姆斯（Ralph Droms），拉爾斯·艾格特（Lars Eggert），吉姆·蓋蒂（Jim Gettys），奧拉維爾·古德蒙森（Olafur Gudmundsson），沃西姆·哈達德（Wassim Haddad），喬爾·M·哈珀恩（David Harrington），李·霍華德，李·霍華德，雷·亨特（Joel Jaeggli），希瑟·柯克西（Heather Kirksey），特德·檸檬（Ted Lemon），阿西·林德姆（Joe Jaeggli），凱里·林恩（Daniel Migault），Erik Nordmark，Michael Richardson，Mattia Rossi，Barbara Stark，Sander Steffann，Markus Stenberg，Don Sturek，Andrew Sullivan，Dave Taht，Dave Thaler，Michael Thomas，Mark Townsley，JP Vasseur，Curtis Villamizar，Russ White，Dan Wing 和 James Woodyatt 在 homenet 工作組會議和工作組郵件

列表中的評論和貢獻。確認通常是指某人的文本將其包含在文件中，或者有助於澄清或增強文件的某個方面。這並不意味著每個貢獻者都同意文件中的每個觀點。

作者資訊

Tim Chown (編輯)
南安普敦大學
Highfield
Southampton, Hampshire SO17 1BJ
United Kingdom
電子郵件：tjc@ecs.soton.ac.uk

Jari Arkko
愛立信
Jorvas 02420
Finland
電子郵件：jari.arkko@piuha.net

Anders Brandt
Sigma 設計
Emdrupvej 26A，1
Copenhagen DK-2100
Denmark
電子郵件：anders_brandt@sigmadesigns.com

Ole Troan
思科系統公司
Philip Pedersensvei 1
Lysaker, N-1325
Norway
電子郵件：ot@cisco.com

Jason Weil
時代華納有線
13820 Sunrise Valley Drive
Herndon, VA 20171
United States
電子郵件：jason.weil@twcable.com