TRUNG TÂM INTERNET VIỆT NAM

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

Trụ sở chính tại TP. Hà Nội:

Tòa nhà VNTA, đường Dương Đình Nghệ,
P. Yên Hòa, Q. Cầu Giấy, Hà Nội
Tel: 024 3556 4944

Fax: 024 3782 1462
Email: info@vnnic.vn
Website: https://vnnic.vn

Chi nhánh tại TP. Đà Nẵng:

Lô 21, Đường số 7, KCN An Đồn
Q. Sơn Trà, TP. Đà Nẵng
Tel: 0236 384 3043

Chi nhánh tại TP. Hồ Chí Minh:

Đường số 20 - Khu chế xuất Tân Thuận
Q. 7, TP. Hồ Chí Minh
Tel: 028 3911 0449

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

Internet Address

TÀI LIỆU
HƯỚNG DẪN TRIỂN KHAI IPV6 CHO 5G, IOT

BỘ THÔNG TIN VÀ TRUYỀN THÔNG
TRUNG TÂM INTERNET VIỆT NAM

TÀI LIỆU
HƯỚNG DẪN TRIỂN KHAI IPV6 CHO 5G, IOT

(Tài liệu dành cho các doanh nghiệp cung cấp dịch IoT, 5G)

Hà Nội, năm 2022

MỤC LỤC

DANH MỤC HÌNH VẼ

LỜI NÓI ĐẦU

Theo số liệu của ITU, năm 2021, 70% dân số thế giới truy cập Internet. Internet đang tiến triển sang giai đoạn tiếp theo, trở thành một thế giới của các thiết bị thông minh có trang bị cảm biến được nối mạng, chia sẻ thông tin với nhau mà không cần sự can thiệp của con người, được gọi là Internet của Vạn vật (Internet of Things - IoT). Theo dự báo, tổng số thiết bị được kết nối Internet of Things lên tới 30,9 tỷ đơn vị trên toàn thế giới vào năm 2025. Với lượng địa chỉ lớn gần như không giới hạn và ưu điểm về công nghệ, IPv6 được khẳng định là giải pháp tối ưu, cung cấp hạ tầng hoàn hảo để phát triển 5G, IoT.

Tại Việt Nam, Kế hoạch hành động quốc gia về IPv6 được thực hiện từ 2011 – 2019. Nhờ các hoạt động đi tắt đúng đầu, triển khai sớm và đúng hướng, Việt Nam đang nằm trong top 10 quốc gia có mức độ sử dụng IPv6 trên Internet cao nhất toàn cầu. Tính đến tháng 8/2022, tỷ lệ ứng dụng IPv6 Việt Nam đạt khoảng 50%, đứng thứ 2 ASEAN, thứ 10 toàn cầu. Mạng Internet Việt Nam đã được chuyển đổi sang thế hệ mới sử dụng địa chỉ IPv6 một cách an toàn, ổn định. Mặc dù vậy, IPv6 cho 5G, IoT và việc ứng dụng IPv6 cho 5G, IoT tại Việt Nam vẫn còn rất mới mẻ.

Việt Nam đang nỗ lực bứt phá trong xu thế số hóa và triển khai dịch vụ mới nhằm đón đầu kỷ nguyên công nghệ mạng. Phát triển hạ tầng kết nối mạng Internet vạn vật (IoT) đã được xác định là nội dung trong phát triển hạ tầng số, là nhiệm vụ, giải pháp tạo nền móng chuyển đổi số tại Chương trình chuyển đổi số quốc gia tới năm 2025, định hướng đến năm 2030 ban hành theo Quyết định số 749/QĐ-TTg ngày 03/6/2020 của Thủ tướng Chính phủ. Các doanh nghiệp Việt Nam cũng đang nỗ lực đi đầu trong cung cấp dịch vụ mới như 5G, IoT.

Tài liệu cẩm nang tổng hợp các thông tin về hiện trạng chuyển đổi Internet thế hệ mới hoạt động với IPv6 trên toàn cầu; hiện trạng và hướng dẫn triển khai ứng dụng IPv6 cho IoT, 5G. Mục tiêu cẩm nang là tài liệu tham khảo cho các tổ chức, doanh nghiệp Việt Nam trong chuyển đổi IPv6 cho dịch vụ Internet mới 5G, IoT.

PHẦN 1: CÁC KHÁI NIỆM, CÔNG NGHỆ CƠ BẢN VỀ IPV6 CHO IOT, 5G

1.1. Các khái niệm cơ bản

IPv6 là gì?

IPv6 là thế hệ địa chỉ Internet phiên bản 6, là thế hệ địa chỉ Internet mới. IPv6 được thiết kế với không gian 128 bít, không gian gần như vô hạn. IPv6 đảm bảo nhu cầu phát triển Internet với các dịch vụ Internet mới như IoT, 5G, Cloud, …

Internet of Things (IoT) là gì?

Internet đang tiến triển thành một thế giới của các thiết bị thông minh có trang bị cảm biến được kết nối mạng, chia sẻ thông tin với nhau mà không cần sự can thiệp của con người, được gọi là Internet của vạn vật (Interne of Things - IoT). IoT là một hệ sinh thái bao gồm tất cả các khía cạnh của Internet, phát triển dựa trên sự hội tụ của công nghệ không dây, công nghệ vi cơ điện tử và Internet.

Mạng 5G là gì?

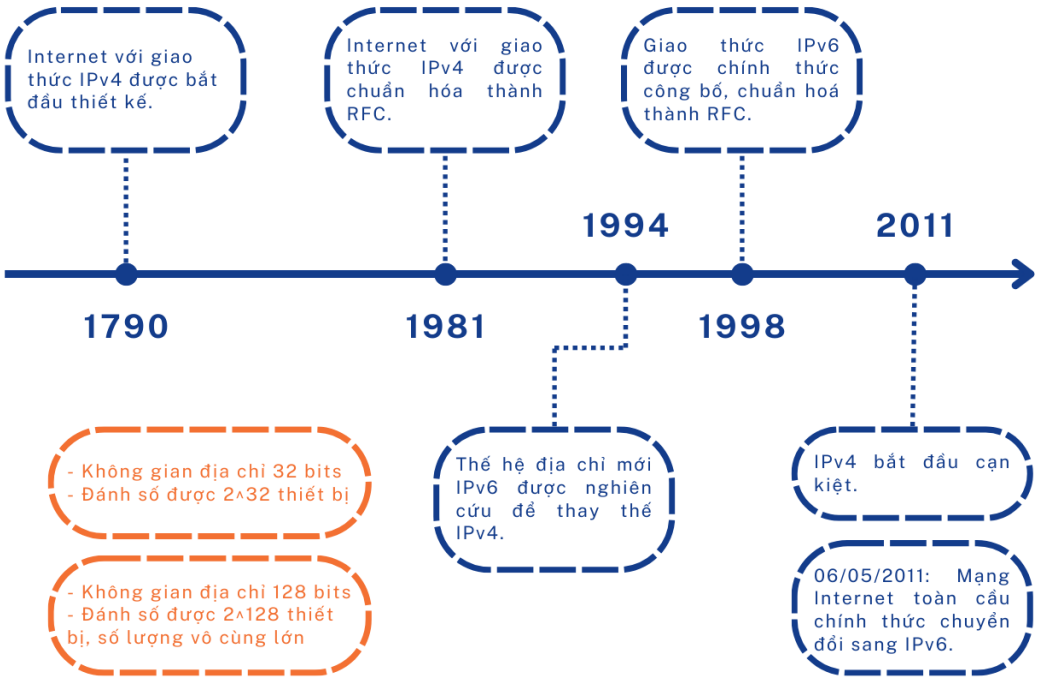
Mạng 5G là thế hệ mạng thứ 5, đáp ứng các yêu cầu cao hơn của một xã hội di động, được kết nối vạn vật. Với sự phát triển của Internet, chuyển đổi số, các ứng dụng được phát triển mạng và lấy con người là trung tâm. Mạng 5G hỗ trợ nhu cầu giao tiếp giữa các ứng dụng, giữa thiết bị với thiết bị, giữa con người với con người. Giúp cuộc sống thuận tiện, an toàn và hiệu quả cao.

1.2. Hiện trạng chuyển đổi IPv6 trên thế giới, Việt Nam

1.2.1. Hiện trạng chuyển đổi IPv6 trên thế giới

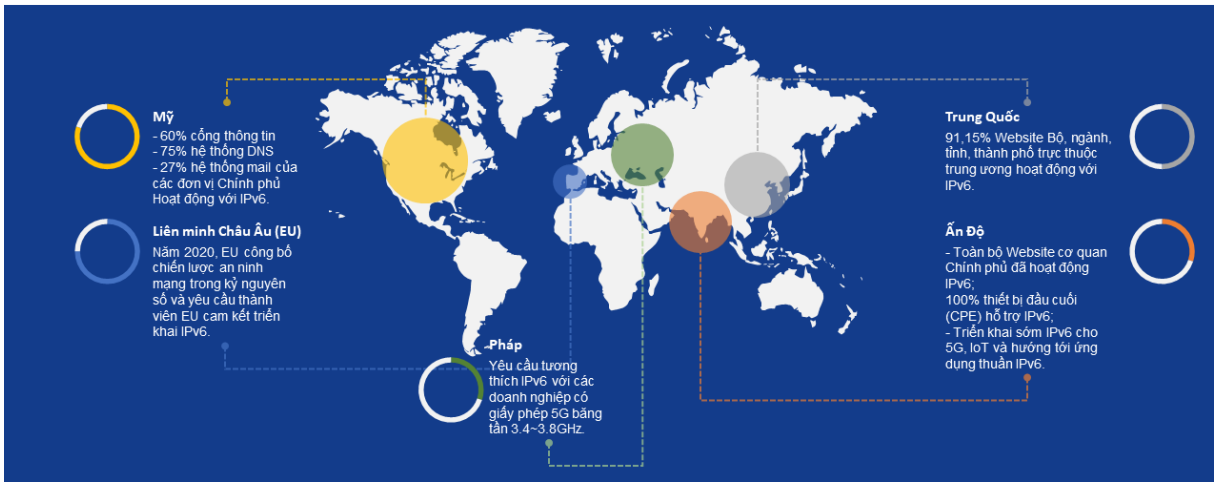
Internet với giao thức IPv4 được bắt đầu thiết kế từ năm 1790 và chính thức chuẩn hoá thành RFC vào năm 1981. Với không gian địa chỉ hạn chế 32 bit, IPv4 bắt đầu cạn kiệt từ năm 2011. Thế hệ địa chỉ mới IPv6 được nghiên cứu từ năm 1994 để thay thế IPv4. Năm 1998, giao thức IPv6 được chính thức công bố, chuẩn hoá thành RFC với không gian địa chỉ 128 bits.

Mạng Internet toàn cầu chính thức chuyển đổi sang IPv6 vào ngày 6/5/2011 với sự tham gia của các công ty lớn như Google, Facebook, Apple, Amazon, AT&T, Comcast, T-Mobile, Verizon Wireless … Từ năm 2008, nhiều quốc gia đã xây dựng và thực hiện kế hoạch chuyển đổi Internet sang IPv6 theo lộ trình chung của thế giới.



Hình 1 Lộ trình chuyển đổi IPv6 toàn cầu

Sau 10 năm chính thức khai trương IPv6 toàn cầu (World IPv6 Launch 2012), tính đến tháng 6/2022, tỷ lệ sử dụng IPv6 bình quân toàn cầu đạt 40% (nguồn Google), 31% (nguồn APNIC). Mạng Internet toàn cầu tiếp tục gia tốc chuyển đổi IPv6 thay thế IPv4 và triển khai IPv6 trong các dịch vụ mới, chất lượng cao như IoT, Smart City, 4G, 5G, Cloud. Xu thế chuyển đổi từ công nghệ song song (dual-stack IPv4/IPv6) sang công nghệ thuần IPv6 (IPv6-only) cũng rõ rệt hơn. Trên các diễn đàn quốc tế, khái niệm IPv6+ được đề cập và thảo luận rộng rãi (kết hợp IPv6 với công nghệ AI, tự động hóa, kết nối Internet với băng thông cực cao, độ trễ thấp, chất lượng cao, bảo mật tốt).



Hình 2 Hiện trạng chuyển đổi IPv6 toàn cầu

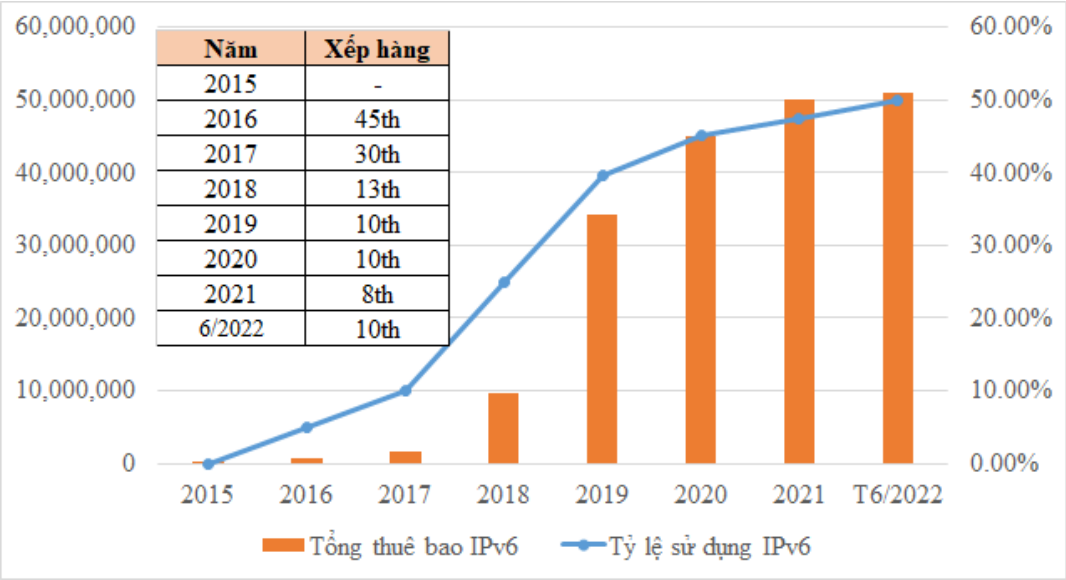
Xếp hạng	Quốc gia	Tỷ lệ sử dụng IPv6
1	Ấn Độ	76.19%
2	Bỉ	66.46%
3	Malaysia	61.22%
4	Ả Rập Xê út	58.99%
5	Uruguay	56.10%
6	Đức	55.34%
7	Sri Lanka	55.11%
8	Hy Lạp	54.81%
9	Hoa Kỳ	51.63%
10	**Việt Nam**	**50.00%**

Bảng 1: Top 10 quốc gia, vùng lãnh thổ về mức độ sử dụng IPv6 (nguồn APNIC)

1.2.2 Chuyển đổi Internet Việt Nam sang IPv6

Đón trước xu thế phải chuyển đổi sử dụng IPv6, Bộ TTTT đã sớm triển khai các hoạt động thúc đẩy chuyển đổi Internet Việt Nam sang IPv6, ban hành và triển khai thành công Kế hoạch hành động quốc gia về IPv6 (2011 - 2019).

Tháng 6/2022, tỷ lệ người sử dụng Internet qua IPv6 đạt 50%, gấp 1,6 lần bình quân toàn cầu. Việt Nam hiện đứng thứ 2 ASEAN (sau Malaysia), thứ 10 toàn cầu; với hơn 50 triệu thuê bao IPv6 (FTTH, Mobile). Việt Nam đã chuyển đổi thành công Internet sang IPv6, là một trong những quốc gia đi đầu, cùng nhịp với các quốc gia lớn trong chuyển đổi IPv6 trên toàn cầu.



Hình 3 Kết quả chuyển đổi Internet Việt Nam sang IPv6

Với mục tiêu định hướng, thúc đẩy, hỗ trợ các cơ quan nhà nước chuyển đổi thành công IPv6 cho hệ thống mạng, dịch vụ công nghệ thông tin, đảm bảo phát triển

hạ tầng số, phục vụ công cuộc chuyển đổi số quốc gia, ngày 14/01/2021, Bộ Thông tin và Truyền thông đã ban hành, công bố "Chương trình thúc đẩy, hỗ trợ chuyển đổi IPv6 cho cơ quan nhà nước giai đoạn 2021 - 2025" (Chương trình IPv6 For Gov).

- Kế hoạch: Đã có 14/22 Bộ, ngành và 62/63 tỉnh, thành phố ban hành Kế hoạch chuyển đổi IPv6 (tổng: 76 Bộ, ngành, địa phương; tăng 72,7% so với cùng kỳ năm trước và tăng 7% so với hết năm 2021).

- Chuyển đổi IPv6 cho Cổng thông tin điện tử, cổng dịch vụ công: 08/22 Bộ, ngành và 33/63 tỉnh thành phố đã chuyển đổi thành công IPv6 cho Cổng Thông tin điện tử, dịch vụ công (đạt 41 Bộ, ngành, địa phương, tăng 141% so với cùng kỳ năm trước và tăng 86% so với hết năm 2021).

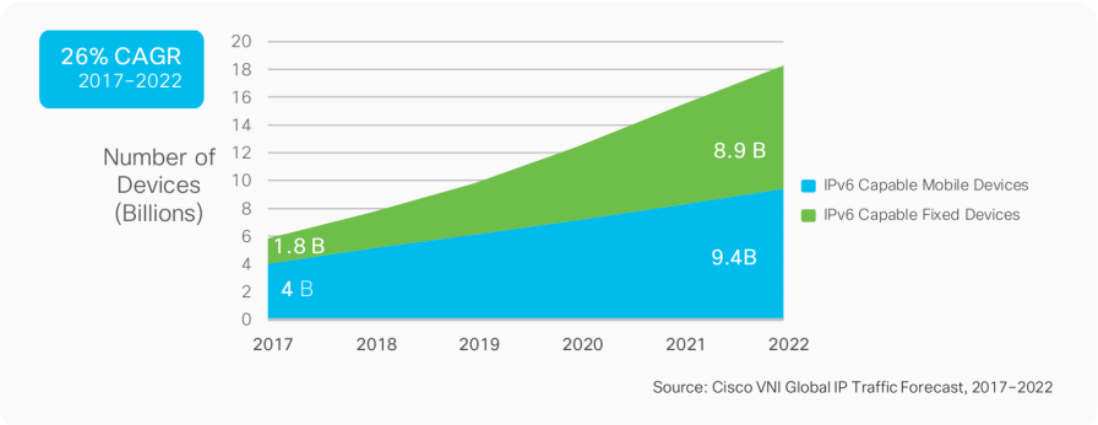
Để phát triển hạ tầng số, nội dung "Chuyển đổi toàn bộ mạng Internet Việt Nam sang ứng dụng địa chỉ giao thức Internet thế hệ mới (IPv6)" đã được xác định trong Chương trình chuyển đổi số quốc gia đến năm 2025, định hướng đến năm 2030 ban hành theo Quyết định số 749/QĐ-TTg ngày 03/6/2020 của Thủ tướng Chính phủ.

1.2.3. IPv6 – Giao thức Internet mặc định dành cho 5G, IoT

Trong những thập kỷ qua, giao thức Internet phiên bản 4 (IPv4) được ứng dụng là giao thức chính cho lớp mạng. Tuy nhiên, giao thức này không được thiết kế cho Internet of Things (IoT), bị giới hạn ở khối lượng hạn chế khoảng 4 tỷ địa chỉ và đã cạn kiệt ở cấp độ toàn cầu vào ngày 3/2/2011. Giao thức mạng IPv6 ra đời nhằm thay thế IPv4 tiếp nối các hoạt động Internet. Bên cạnh việc thay thế cho IPv4 đã cạn kiệt, các tính năng được thiết kế nâng cấp của IPv6 rất phù hợp và mang lại lợi thế cho IoT, 5G.

Cisco đã công bố số liệu dự báo số lượng thiết bị hỗ trợ IPv6 tăng từ 6 tỷ vào năm 2017 lên 18,3 tỷ vào năm 2022 (Cisco's Visual Networking Index: Forecast and Trends, 2017-2022).

Figure 8. Global IPv6-capable devices and connections forecast, 2017–2022



Hình 4 Sự tăng trưởng về số lượng thiết bị IPv6 trên Internet

Đặc tính của IPv6 giúp phát triển IoT, 5G:

• Khả năng mở rộng: IPv6 có không gian địa chỉ khổng lồ. Không gian 2^{128} (3,4 × 10^38) địa chỉ IPv6 đủ để giải quyết nhu cầu của tất cả thiết bị giao tiếp hiện tại và tương lai, cho phép mở rộng kết nối Internet tới bất kỳ thiết bị và dịch vụ nào.

• Giải quyết rào cản NAT: IPv6 hỗ trợ kết nối đầu cuối-đầu cuối và loại bỏ hoàn toàn công nghệ NAT.

• Cải thiện về định tuyến: Định tuyến IPv6 được thiết kế hoàn toàn phân cấp.

• Tự động cấu hình địa chỉ không trạng thái Stateless (SLAAC): IPv6 được thiết kế với khả năng tự động cấu hình mà không cần sử dụng máy chủ DHCP, hỗ trợ hơn nữa trong việc giảm cấu hình thủ công; phù hợp với mạng IoT, 5G.

• Multicast và Anycast: Multicast có được hỗ trợ trong IPv4 nhưng không hiệu quả trong thực tế nên hầu như không được sử dụng. Các thành phần quan trọng của Internet dễ gặp rủi ro khi sử dụng multicast IPv4. Với IPv6, việc sử dụng multicast hạn chế rủi ro hơn rất nhiều nhờ vào việc quy hoạch địa chỉ cho các nhóm điểm đến. IPv6 multicast đặc biệt hữu ích trong môi trường IoT, đặc biệt trong các mạng IoT quy mô lớn. Anycast không được thiết kế trong IPv4. IPv6 Anycast rất hữu ích trong mạng cục bộ và mạng cảm biến.

• Chất lượng dịch vụ: Cấu trúc địa chỉ IPv6 cung cấp một số bit để xác định mức Chất lượng dịch vụ (QoS) trong xử lý các gói tin.

• Tính di động: IPv6 cung cấp các tính năng và giải pháp mạnh mẽ để hỗ trợ tính di động của cả nút đầu cuối và các nút định tuyến. IPv4 cũng cung cấp tính di động nhưng giao thức Internet di động (MIP) mà IPv4 sử dụng rất không hiệu quả: khi mỗi gói tin phải đi qua Home Agent bằng đường dẫn hình tam giác. Trong IPv6, một phiên bản mới của MIP là MIPv6 đã được phát triển. So với MIP, MIPv6 giảm độ trễ chuyển giao nhờ một số tối ưu hóa trong các cơ chế: phát hiện chuyển động (MD); phát hiện địa chỉ trùng lặp (DAD) và Cập nhật ràng buộc (BU).

• Bảo mật: Thiết kế của IPv4 không tính đến vấn đề bảo mật. Do đó, bảo mật trong IPv4 phải được thực hiện bằng các ứng dụng. Để khắc phục hạn chế này, tính năng bảo mật được thiết kế trong IPv6, có thể kể tới gồm IPSec cho thiết bị đầu cuối, cho di động, Giao thức Neighbor Discovery (NDP).

Với thiết kế nêu trên, IPv6 được xác định là giao thức Internet mặc định cho dịch vụ Internet mới như 5G và IoT.

1.3. Các tiêu chuẩn, công nghệ cơ bản về IPv6 cho 5G, IoT

1.3.1. Các tiêu chuẩn, công nghệ cơ bản về IPv6 cho IoT

a) Một số công nghệ, kỹ thuật truyền tải trong IoT

- **Bluetooth / BLE:** Bluetooth hoặc công nghệ Bluetooth năng lượng thấp (Bluetooth Low Energy – BLE) là tiêu chuẩn cho phép kết nối các thiết bị điện năng thấp và cảm biến, sử dụng truyền dẫn vô tuyến bước sóng ngắn, băng tần 2.4GHz. Hiện nay, BLE - Bluetooth Low Energy - hoặc Bluethooth Smart là một giao thức được sử dụng đáng kể cho các ứng dụng IoT.

- **Zigbee**: Giống như Bluetooth, là một loại truyền thông trong khoảng cách ngắn, hiện được sử dụng với số lượng lớn và thường được sử dụng trong công nghiệp. Điển hình, Zigbee Pro và Zigbee remote control (RF4CE) được thiết kế trên nền tảng giao thức IEEE802.15.4 - là một chuẩn giao thức truyền thông vật lý trong công nghiệp hoạt động ở 2.4Ghz.

- **Z-Wave**: Tương tự Zigbee, Z-Wave là chuẩn truyền thông không dây trong khoảng cách ngắn và tiêu thụ rất ít năng lượng. Chuẩn kết nối Z-Wave và Zigbee cùng hoạt động với tần số 2.4GHz, và cùng được thiết kế với mức tiêu thụ năng lượng rất ít nên có thể sử dụng với các loại PIN di động.

- **NFC:** (Near-Field Communications) là công nghệ kết nối không dây trong phạm vi tầm ngắn trong khoảng cách 4 cm. Công nghệ này sử dụng cảm ứng từ trường để thực hiện kết nối giữa các thiết bị (smartphone, tablet, loa, tai nghe …) khi có sự tiếp xúc trực tiếp.

- **Sigfox:** là hệ thống giống như mạng di động, sử dụng công nghệ Ultra Band (UNB) để kết nối các thiết bị từ xa. Mục tiêu của công nghệ là sử dụng trong các ứng dụng truyền thông với tốc độ thấp, khoảng cách truyền xa và mức tiêu thụ năng lượng cực thấp. Sigfox sử dụng các dải tần ISM được sử dụng miễn phí mà không cần phải được cấp phép để truyền dữ liệu.

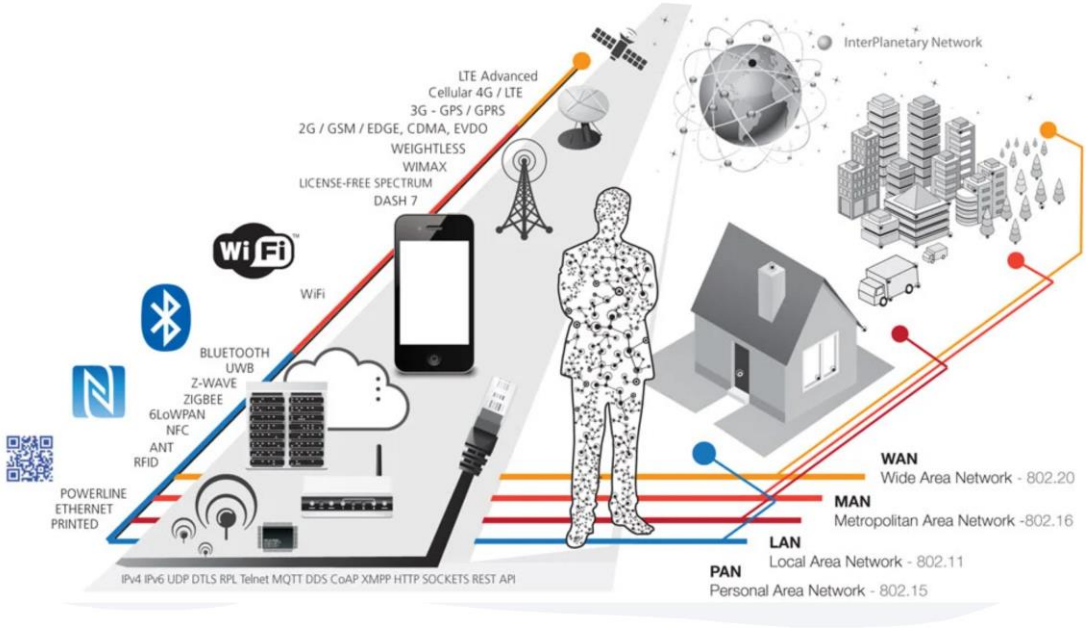
- **Neul:** Tương tự Sigfox và hoạt động ở băng tần 1Ghz, với mục tiêu cung cấp một mạng không dây có chi phí thấp với các đặc trưng tiêu biểu: độ mở rộng cao, phủ sóng cao và tiêu thụ năng lượng cực thấp. Neul sử dụng chip Iceni để truy cập vào băng tần UHF. Tốc độ truyền dữ liệu có thể dao động từ vài bits trên giây tới 100kbps trên cùng một liên kết. Với công nghệ này, thiết bị có thể tiêu thụ công suất rất nhỏ, từ 20 tới 30mA, tức là có thể sử dụng đươc từ 10 đến 15 năm với một pin.

- **Wifi:** (Wireless Fidelity hay mạng 802.11) là hệ thống mạng không dây sử dụng sóng vô tuyến, cũng giống như điện thoại di đông, truyền hình và radio. Các

sóng vô tuyến sử dụng cho WiFi gần giống với các sóng vô tuyến sử dụng cho thiết bị cầm tay, điện thoại di động và các thiết bị khác. Hiện nay, đa số các thiết bị wifi đều tuân theo chuẩn 802.11n, được phát ở tần số 2.4Ghz và đạt tốc độ xử lý tối đa 300Megabit/giây.

- **Di động (Cellular)**: Với các ứng dụng IoT/M2M yêu cầu khoảng cách truyền thông dài, hoặc không bị giới hạn bởi khoảng cách địa lý thì việc lựa chọn đường truyền dữ liệu thông qua mạng điện thoại di động GPRS/3G/LTE là một lựa chọn tối ưu. Tuy nhiên truyền dữ liệu đi xa phải chấp nhận yếu tố tiêu hao năng lượng.

- **Thread:** là một giao thức IP mới, dựa trên nền tảng mạng IPv6 được thiết kế riêng cho mảng tự động hóa trong các tòa nhà. Đây không phải là một giao thức được phổ biến như hiện nay để ứng dụng trong IoT như Zigbee hay Bluetooth. Được ra mắt vào giữa năm 2014, giao thức Thread dựa trên các tiêu chuẩn khác nhau, bao gồm IEEE802.15.4, IPv6 và 6LoWPAN, và cung cấp một giải pháp dựa trên nền tảng IP cho các ứng dụng IoT.



Hình 5 Kết nối trong Internet of Things (www.postscapes.com)

- **6LoWPAN:** là giao thức IPv6 trong các mạng không dây công suất thấp. 6LoWPAN được phát triển bởi IETF, cho phép truyền dữ liệu qua các giao thức IPv6 và IPv4 trong các mạng không dây công suất thấp với các cấu trúc mạng điểm - điểm (P2P: point to point) và dạng lưới (mesh). 6LoWPAN được thiết kế để cho phép IPv6 sử dụng rộng rãi trong các ứng dụng IoT.

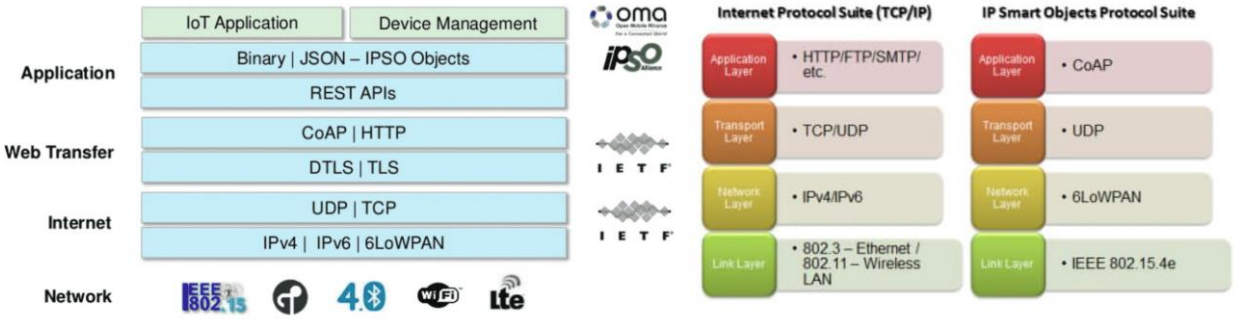
- **IEEE 802.15.4 WPAN:** IEEE 802.15 TG4 được thiết lập để thiết kế giải pháp tốc độ dữ liệu thấp với tuổi thọ pin từ nhiều tháng đến nhiều năm và độ phức tạp rất thấp, hoạt động với băng tần không cấp phép quốc tế. Các ứng dụng tiềm năng là cảm biến, đồ chơi tương tác, thẻ thông minh, điều khiển từ xa và tự động hóa tòa nhà.

- **IEEE 802.11 WLAN** (Mạng cục bộ không dây).

- LPWAN (Low Power and Wide Area Network - Mạng điện năng thấp và diện rộng).

- Mạng di động (NB-IoT, 5G).

b) Các tiêu chuẩn sử dụng trong IoT



Hình 6 Khái quát hóa cấu trúc và ngăn xếp thủ tục dành cho IoT

IoT là một mô trường phức hợp, đa dạng và hiện có rất nhiều tiêu chuẩn khác nhau, có thể liệt kê theo các lĩnh vực như sau:

- Hạ tầng (Infrastructure): 6LowPAN, IPv4/IPv6, RPL.

- Định danh (Identification): EPC, uCode, IPv6, URIs.

- Giao tiếp / Truyền tải (Comms / Transport): Wifi, Bluetooth, LPWAN.

- Khám phá (Discovery): Physical Web, mDNS, DNS-SD.

- Giao thức dữ liệu (Data Protocols): MQTT, CoAP, AMQP, Websocket, Node.

- Quản lý thiết bị (Device Management): TR-069, OMA-DM.

- Định dạng dữ liệu (Semantic): JSON-LD, Web Thing Model.

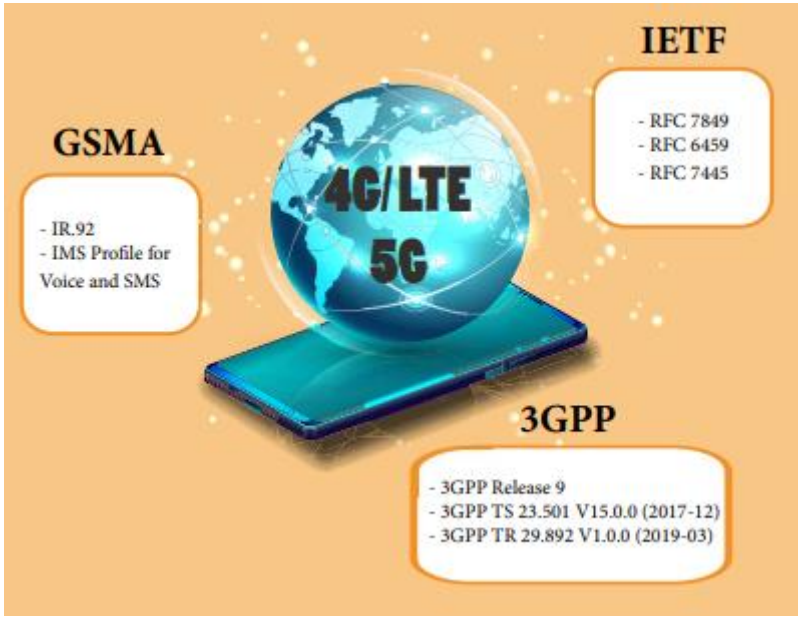
- Multi-layer Frameworks: Alljoyn, IoTivity, Weave, Homekit.

1.3.2. Các tiêu chuẩn, công nghệ cơ bản về IPv6 cho 5G

5G (Thế hệ mạng di động thứ 5 hoặc hệ thống không dây thứ 5) là thế hệ tiếp theo của công nghệ truyền thông di động sau thế hệ 4G, hoạt động ở các băng tần 28,

38, và 60 GHz. Sự khác biệt của mạng 5G: Tốc độ nhanh hơn (gửi được dữ liệu lớn hơn); Độ trễ thấp; Khả năng kết nối nhiều thiết bị (cảm biến và thiết bị thông minh).

Các tiêu chuẩn 4G LTE/ 5G được IETU, 3GPP và GSMA nghiên cứu đưa ra. Các tiêu chuẩn sử dụng để triển khai công nghệ 4G LTE cũng như 5G. Theo đó, IPv6 là giao thức mặc định trong triển khai 4G LTE, 5G.



Hình 7 Các tiêu chuẩn IPv6 cho 4G LTE, 5G

- **IETF:** RFC 7849, RFC 6459, RFC 7445.

- **GSMA**: IR.92; IMS Profile for Voice and SMS.

- **3GPP:** 3GPP Release 9; 3GPPTS 23.501 V15.0.0 (2017-12); 3GPP TR 29.882 V1.0.0 (2019-03).

Ngoài ra, khi triển khai IPv6 cho mạng di động, một số giải pháp công nghệ được áp dụng phổ biến như: Dual-stack, 464XLAT, NAT64.

Country	Transition Mechanism (NAT64/464xlat, 6rd, DS-Lite, Dual Stack, ...)	Network Type (mobile, DSL, fiber, cable, satellite,...)
US	?	Mobile
BT	Dual Stack	Mobile
GB	464XLAT	Mobile
TT	Dual Stack	Mobile
DE	464XLAT, NAT64	mobile (2G,3G,4G)
DE	Dual Stack	mobile (2G,3G,4G)
EE	dual stack	mobile
TW	Dual Stack	Mobile
VN	dual stack	LTE
NO	Dual stack	3GPP
FR	Dual-stack	Mobile
PL	464XLAT	Mobile
IN	464XLAT	Mobile
CA	NAT64/464XLAT	Wireless
US	464XLAT	mobile
US	464XLAT, NAT64	mobile
SE	Dual stack	3GPP
AU	464XLAT	mobile
DK,SE	Dual stack	3GPP
US	Dual-stack	mobile

Việt Nam

Hình 8 Thống kê giải pháp triển khai IPv6 của mạng di động

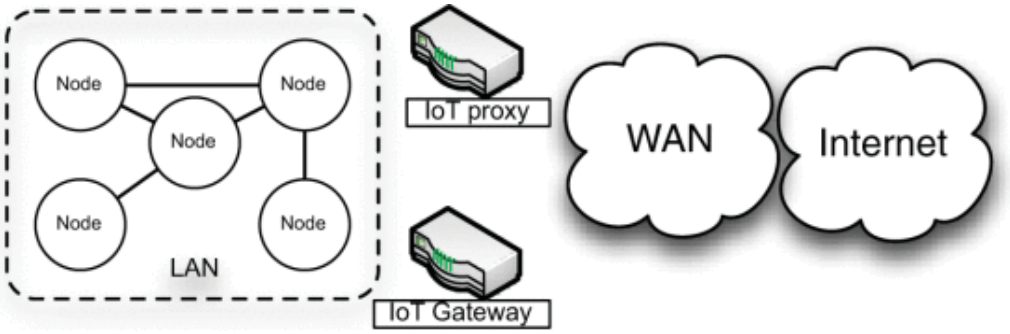
Qua các nội dung công nghệ, tiêu chuẩn cơ bản và thực thiễn cho thấy IPv6 là giao thức Internet với nhiều đặc tính tối ưu về thiết kế, phù hợp với xu thế phát triển; IPv6 là giao thức Internet mặc định cho 5G, IoT.

PHẦN 2: HƯỚNG DẪN TRIỂN KHAI IPv6 CHO IoT

2.1. Mô hình kiến trúc triển khai IPv6 cho IoT

2.1.1. Mô hình kiến trúc IoT

Hình dưới đây mô tả bố cục cấp cao của Internet of Things. Nhìn bề ngoài, kiến trúc không khác với bất kỳ cấu trúc mạng Internet thông thường nào.



Hình 9 Kiến trúc chung của Internet vạn vật.

(1) Nút IoT

Nút IoT là những thứ được kết nối với Internet trực tiếp hoặc gián tiếp thông qua mạng cục bộ IoT (LAN) hoặc WAN. Nếu mạng LAN IoT được kết nối với Internet, nút IoT cũng có thể được kết nối trực tiếp với Internet dù không phải luôn luôn như vậy. Ngoài ra, có những trường hợp nút IoT được kết nối với Internet thông qua kết nối WAN mà không có mạng LAN IoT. Những nút này cần có khả năng tự cấu hình. Các nút IoT có thể được chia lớp khác nhau dựa trên các đặc tính, chẳng hạn như các nút chuyển tiếp, cảm biến / thiết bị truyền động, thiết bị cấp nguồn, thiết bị kết nối.

(2) IoT LAN

IoT LAN là một mạng lưới các nút IoT nằm trong sự kiểm soát của một thực thể và sử dụng phạm vi kết nối các thiết bị để kết nối các nút khác nhau. IoT LAN có thể được cấu hình bằng cách sử dụng mạng khác công nghệ, cấu trúc liên kết và thiết bị kết nối tầm ngắn, công suất thấp. IoT LAN có thể được kết nối với internet thông qua cổng IoT hoặc proxy IoT để cung cấp kết nối toàn cầu đến các nút IoT. Gateway trong mạng LAN có thể được kết nối qua các tín hiệu như điện, sóng radio, sóng âm, sóng từ, quang tín hiệu, tín hiệu hóa học, v.v.

(3) IoT WAN / Internet

Nút IoT hoặc IoT LAN có thể được kết nối trực tiếp với internet hoặc WAN, và sau đó được kết nối với Internet. Mạng diện rộng IoT (WAN) là mạng bao phủ về mặt

địa lý và tổ chức trên diện rộng. Mặc dù các mạng LAN IoT có thể được kết nối trực tiếp với Internet, IoT cũng có thể được coi là một mạng lưới, với các mạng LAN được kết nối và tổng hợp thông qua các mạng WAN sau đó được kết nối với Internet. Do đó, một mạng WAN thường là sự kết hợp của các phân đoạn mạng được quản lý bởi những thực thể khác nhau, có khả năng là một khu vực địa lý rất rộng lớn.

(4) Cổng IoT (IoT gateway) và Proxy

Cổng kết nối IoT là một bộ định tuyến kết nối mạng LAN IoT với mạng WAN và với Internet. Cổng kết nối IoT là một thiết bị lớp 3, chuyển tiếp các gói IP giữa IoT LAN và WAN triển khai cả hai công nghệ mạng. Một cổng kết nối IoT có khả năng triển khai một số công nghệ LAN và WAN (không dây hoặc có dây) tùy thuộc vào cấu hình. Cổng IoT chuyển tiếp các gói giữa IoT LAN và WAN trên lớp IP mà không cần thực hiện các tác vụ lớp ứng dụng. Trong một mạng LAN IoT, có thể không có hoặc nhiều cổng IoT tùy thuộc vào tình huống.

Proxy IoT là một thực thể thực hiện chức năng lớp ứng dụng hoạt động giữa các nút IoT và các thực thể khác. Chức năng của lớp ứng dụng có thể bao gồm từ chuyển đổi giao thức ứng dụng tương đối đơn giản sang các chức năng ứng dụng tích cực hơn. Proxy IoT có thể được kết nối với cổng IoT.

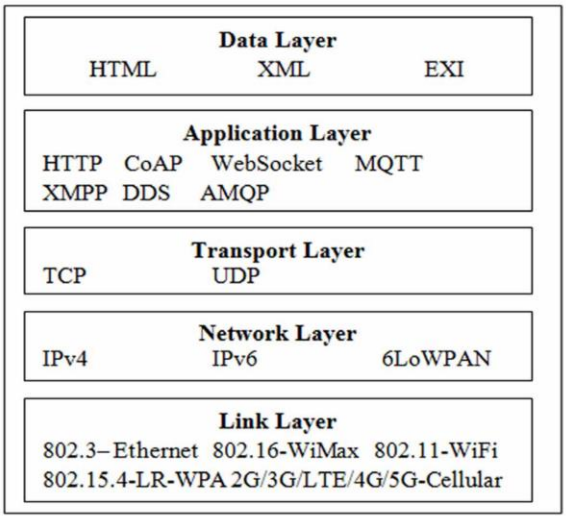
(5) Phương tiện truyền thông

Phương tiện này có thể có dây hoặc không dây. Chức năng chính của phương tiện truyền thông là chuyển thông tin dưới dạng tín hiệu từ một nút đến nút khác hoặc các mạng. Tín hiệu có thể ở bất kỳ dạng nào như điện, sóng vô tuyến, sóng từ, sóng âm thanh, tín hiệu hóa học, v.v.

(6) Bộ định tuyến biên (Egde router)

Bộ định tuyến biên được sử dụng để chuyển đổi địa chỉ IP từ dạng này sang dạng khác và chuyển tiếp dữ liệu gói tin đã nhận. Nhiều nhà nghiên cứu đã đề xuất một kiến trúc giao thức phân lớp khác nhau của IoT. Nhìn chung, ngăn xếp giao thức chung cho các thiết bị IoT đã chia giao thức trong năm lớp chức năng riêng biệt, được đặt tên là (1) Dữ liệu, (2) Ứng dụng, (3) Vận chuyển, (4) Mạng và (5) Lớp liên kết

Figure 2. IoT protocol stack



Hình 10 Ngăn xếp thủ tục IoT

(7) Lớp dữ liệu

Trong dữ liệu IoT được trao đổi bằng cách biểu diễn các nội dung dưới dạng một số đại diện ngữ nghĩa ngôn ngữ, như Ngôn ngữ đánh dấu eXtensible (XML), Ngôn ngữ đánh dấu siêu văn bản (HTML) cho các nút không bị giới hạn và Trao đổi XML hiệu quả (EXI) vốn được sử dụng rộng rãi cho các nút hạn chế.

(8) Lớp ứng dụng

Lớp này cung cấp một giao diện ứng dụng với lớp truyền tải để truyền dữ liệu lên Internet. Giao thức HTTP thường được sử dụng để mã hóa dữ liệu lớp ứng dụng, nhưng HTTP không thích hợp đối với các nút hạn chế. CoAP (Constrained Application Protocol) được sử dụng trong môi trường các nút hạn chế và truyền dữ liệu và sử dụng UDP thay vì TCP. Các giao thức lớp ứng dụng khác được sử dụng trong các ứng dụng cụ thể như Message Queue Telemetry Transport (MQTT), Extensible Messaging and Presence Protocol (XMPP), Data Distribution Service (DDS), and Advanced Message Queuing Protocol (AMQP).

(9) Lớp vận chuyển

Chức năng chính của lớp vận chuyển là cung cấp phân phối dữ liệu từ đầu đến cuối. Giao thức điều khiển truyền (TCP) và UDP được sử dụng để phân phối dữ liệu từ một điểm cuối này đến điểm cuối khác.

(10) Lớp mạng

Đây là yêu cầu cơ bản để gắn địa chỉ duy nhất cho nút IoT và định tuyến các gói dữ liệu qua Internet. Trong IoT, hàng nghìn tỷ thiết bị yêu cầu địa chỉ IP duy nhất.

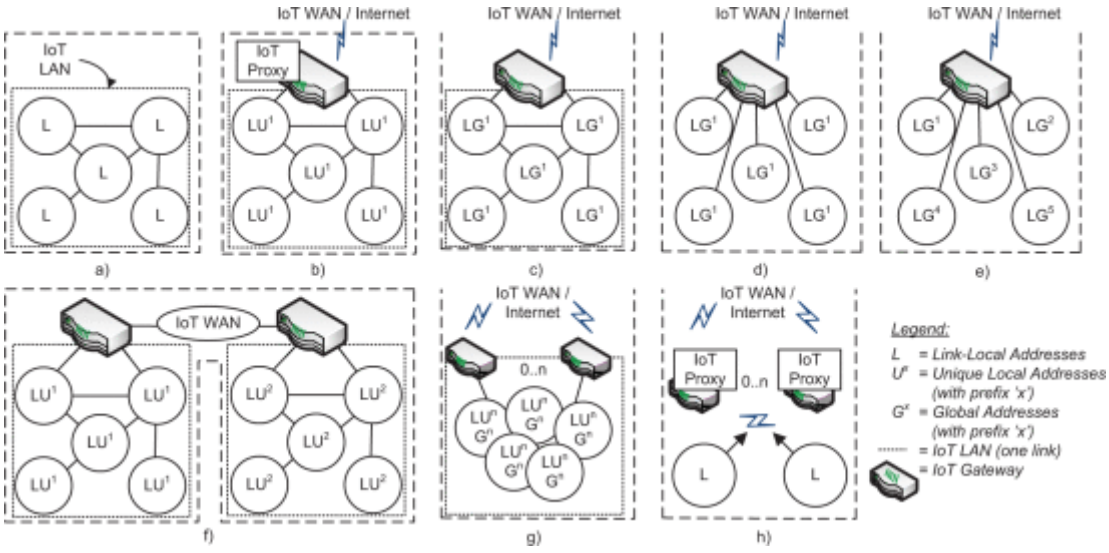
Do IPv4 cạn kiệt, IPv6 sẽ đủ không gian để cung cấp địa chỉ duy nhất cho hàng tỷ nút IoT. Mặc dù giải quyết vấn đề về không gian địa chỉ nhưng với chiều dài 128 bit, IPv6 gây quá tải và không phù hợp với các nút IoT hạn chế. Vấn đề này được khắc phục bằng Giao thức 6LoWPAN là một dạng nén của IPv6. Một bộ định tuyến biên được sử dụng để dịch địa chỉ từ IPv6 sang 6LoWPAN và ngược lại.

(11) Lớp liên kết

Lớp liên kết chịu trách nhiệm gửi dữ liệu qua phương tiện vật lý của mạng. Các giao thức của lớp liên kết trong môi trường IoT có thể là 802.3 Ethernet, 802.11 WI-FI, 802.16- WiMAX, 802.15.4 tốc độ thấp mạng cá nhân không dây (LR-WPANs) và mạng di động 2G / 3G / LTE / 4G / 5G…

2.1.2. Cấu trúc triển khai các mạng IoT

Các cấu trúc triển khai mạng IoT được minh họa trong các hình dưới đây. Các cấu trúc liên kết này có thể được mở rộng thành các cấu trúc liên kết phức tạp hơn với các biến thể.



Hình 11 Các mô hình thiết lập LAN IoT

(1) Mạng IoT không kết nối và không có nút trung tâm

Mạng LAN IoT bị ngắt kết nối có thể không có kết nối Internet và chỉ có kết nối trong liên kết của mình. Cấu trúc kết nối có thể dạng lưới, hình sao hoặc kết nối chia sẻ, nhưng tuy nhiên, các nút thông minh IPv6 nằm trong một liên kết duy nhất mà không cần bất kỳ bộ định tuyến nào. Do đó, không có thực thể nào trong mạng có thể cung cấp một tiền tố ULA hoặc GUA. Trong loại cấu trúc liên kết này, yêu cầu cơ bản để giải quyết là các nút IoT phải có khả năng tự động đánh số. Vì việc đánh số tự động trong một số trường hợp phải rất đơn giản, các địa chỉ IPv6 có thể được cấu hình tĩnh. Địa chỉ

có thể định tuyến là không cần thiết vì mạng này không được kết nối với các mạng khác cũng như nối Internet. Do đó, loại địa chỉ phù hợp nhất là địa chỉ IPv6 link-local.

(2) Mạng có proxy IoT

Trong trường hợp này, IoT LAN đã được tăng cường với một proxy IoT, có thể cung cấp địa chỉ và có thể là các dịch vụ kết nối cho các nút IoT trong IoT LAN. Proxy IoT có thể có kết nối vĩnh viễn hoặc không liên tục với mạng bên ngoài hoặc trong một số trường hợp là không có kết nối. Khi proxy IoT có kết nối đường lên, nó ủy quyền giao tiếp giữa các nút IoT cục bộ và các nút trong mạng bên ngoài. Trong trường hợp này, khi tất cả thông tin liên lạc đi qua proxy, IoT LAN không cần địa chỉ toàn cầu, nhưng có thể quản lý bằng địa chỉ liên kết cục bộ hoặc địa chỉ ULA, tùy thuộc vào loại proxy.

(3) Mạng IoT được kết nối

Đây là thiết lập điển hình để cung cấp các nút IoT có kết nối Internet. Cổng IoT được kết nối Internet cung cấp kết nối Internet với mạng LAN IoT. Cổng kết nối IoT nhận tiền tố IPv6 có thể định tuyến toàn cầu từ nhà cung cấp dịch vụ Internet và sử dụng tiền tố đó để đánh số các nút trong mạng LAN IoT. Có các cơ chế khác nhau để lấy tiền tố IPv6 cho phép các nút IoT trong mạng LAN được cung cấp địa chỉ có thể định tuyến toàn cầu. Ngoài ra, các nút IoT, chỉ giao tiếp trong liên kết của riêng chúng, có thể sử dụng địa chỉ liên kết cục bộ và cổng IoT cũng có thể cung cấp địa chỉ ULA cho các nút IoT.

(4) Mạng IoT với cấu trúc liên kết hình sao

Trong một số trường hợp, thiết bị cổng (gateway) là trung tâm của mạng sử dụng cấu trúc liên kết hình sao. Trong một mạng như vậy, một tiền tố IPv6 có thể được chia sẻ bởi các nút được kết nối thông qua các liên kết điểm-điểm thông qua thiết bị cổng và cổng đóng vai trò cầu nối. Cách tiếp cận này được sử dụng trong tiêu chuẩn IETF phát triển trên đường truyền IPv6 qua Bluetooth năng lượng thấp. Ngoài ra, các kịch bản triển khai IoT cũng tồn tại mô phỏng cấu trúc liên kết hình sao bắc cầu, nhưng chỉ có cổng duy trì IPv6 cho các nút IoT cực kỳ đơn giản không triển khai IPv6. Ví dụ: cảm biến kết nối và giao tiếp với cổng IPv6 bằng 1 dây hoặc giải pháp tương tự mà không nhận biết IPv6. Tuy nhiên, cổng phân bổ địa chỉ IPv6 và duy trì nội bộ IPv6 1: 1 tới ánh xạ mã định danh độc quyền cho mỗi nút.

(5) Mạng điểm-điểm với cổng Internet

Mạng điểm – điểm với cổng Internet rất giống với mạng IoT với cấu trúc liên kết hình sao ngoại trừ việc các nút IoT không nằm trên cùng một liên kết. Thay vào

đó, chúng được kết nối với IoT Gateway thông qua các liên kết của riêng chúng. Do đó, không thể giao tiếp bằng cách sử dụng địa chỉ liên kết cục bộ giữa các nút IoT.

(6) Mạng IoT được kết nối với nhau

Khi nói đến các kịch bản nâng cao hơn, hai hoặc nhiều mạng LAN IoT có thể được kết nối với nhau thông qua liên kết được chia sẻ hoặc thông qua IoT WAN. Trong trường hợp này, các nút IoT của các mạng LAN khác nhau rõ ràng không nằm trên một liên kết được chia sẻ với nhau. Do đó, giao tiếp giữa chúng không thể thực hiện được với các địa chỉ liên kết cục bộ. Nếu các nút IoT cần giao tiếp với các nút trên các phân đoạn mạng khác nhau, địa chỉ được sử dụng phải là ULA hoặc GUA, tùy thuộc vào mạng nằm giữa các cổng. Nếu mạng là Internet, địa chỉ IPv6 có thể định tuyến toàn cầu phải được sử dụng trong mạng. Trong trường hợp không phải lúc nào cũng có kết nối Internet, cả hai phạm vi địa chỉ đều có thể được sử dụng.

(7) Nhiều cổng

Các cấu trúc liên kết được mô tả trên đại diện cho các cấu trúc liên kết cơ bản. Tuy nhiên, có những biến thể của các cấu trúc liên kết cơ bản cần có các kịch bản đánh địa chỉ khác. Ví dụ: có thể có nhiều cổng kết nối mạng LAN IoT với Internet hoặc với Internet và mạng diện rộng riêng — chẳng hạn như mạng công ty — do đó, làm cho IoT LAN trở nên đa năng. Nếu các nút IoT cần có thể truy cập được từ cả hai mạng, thì các nút IoT cần có địa chỉ từ cả hai mạng. Do đó, các nút IoT có thể cần có nhiều địa chỉ trên phạm vi toàn cầu.

(8) Các nút IoT một chiều

Trong mạng IoT có thể có các liên kết một chiều, hay nói cách khác là có các nút IoT chỉ gửi. Cách tiếp cận đơn hướng không hoàn toàn tương thích với các giải pháp định địa chỉ IPv6 hiện có, vì tất cả các giải pháp đó đều sử dụng truyền thông hai chiều để thực hiện thủ tục Phát hiện địa chỉ trùng lặp và cho các giao tiếp khác. Trong các trường hợp có nút IoT một chiều như thế này, vẫn có thể sử dụng IPv6. Cách để giải quyết các nút trong mô hình triển khai như vậy là tin tưởng các địa chỉ liên kết cục bộ là duy nhất, gắn cứng chúng và sử dụng đia chỉ multicast đa hướng liên kết cục bộ (link-local multicast) làm địa chỉ đích.

(9) Các biến thể của các cấu trúc liên kết cơ bản

Ngoài các biến thể cấu trúc liên kết, các cấu trúc liên kết cũng có thể được kết hợp. Ví dụ: trong cùng một mạng LAN IoT, một số nút có thể được kết nối trực tiếp với Internet bằng các địa chỉ toàn cầu và một số nút có thể sử dụng ULA hoặc địa chỉ liên kết cục bộ để liên lạc cục bộ hoặc giao tiếp thông qua proxy. Trong những trường

hợp này, ngay cả khi các yêu cầu về địa chỉ có thể khác nhau giữa các nút IoT trong cùng một mạng, điều quan trọng cần nhớ là các nút giao tiếp giữa nhau cần phải có địa chỉ có cùng phạm vi.

2.1.3. Nguyên tắc gán địa chỉ IPv6 cho thiết bị IoT

Có ba phương pháp để gán địa chỉ IPv6 cho đầu cuối:

- Gán địa chỉ IPv6 thủ công: Phương pháp này thích hợp cho các máy chủ không bao giờ thay đổi địa chỉ, nhưng không thích hợp cho hàng triệu điểm cuối, chẳng hạn như thiết bị đo, vì liên quan đến chi phí và độ phức tạp.

- Gán địa chỉ IPv6 tự động có trạng thái (stateful addressing): Thông qua việc sử dụng Giao thức điều khiển máy chủ động cho IPv6 (DHCPv6). Phương pháp này có ưu điểm là bảo mật vì quá trình DHCPv6 có thể được kết hợp với xác thực, ủy quyền cộng với hệ thống tên miền (DNS) có sẵn. Tuy nhiên, phương thức này không phù hợp với IoT vì các thiết bị hoặc mạng có thể không hỗ trợ việc duy trì các bảng hoặc Máy chủ DHCP.

Các giao thức trạng thái có thể được chia thành quản lý tập trung và phân tán. Do địa chỉ chi tiết của tất cả các nút IoT trong mạng được lưu trữ trong một hoặc một số nút IoT nên không cần phải có cơ chế phát hiện địa chỉ trùng lặp (DAD). Cơ chế quản lý tập trung sử dụng giao thức DHCP và bảng phân bổ tập trung. Cơ chế quản lý phân tán cho phép mọi nút giữ bảng phân bổ của riêng nó một cách độc lập và cấp phát địa chỉ cho các nút yêu cầu bằng cách trao đổi thông điệp với các nút lân cận.

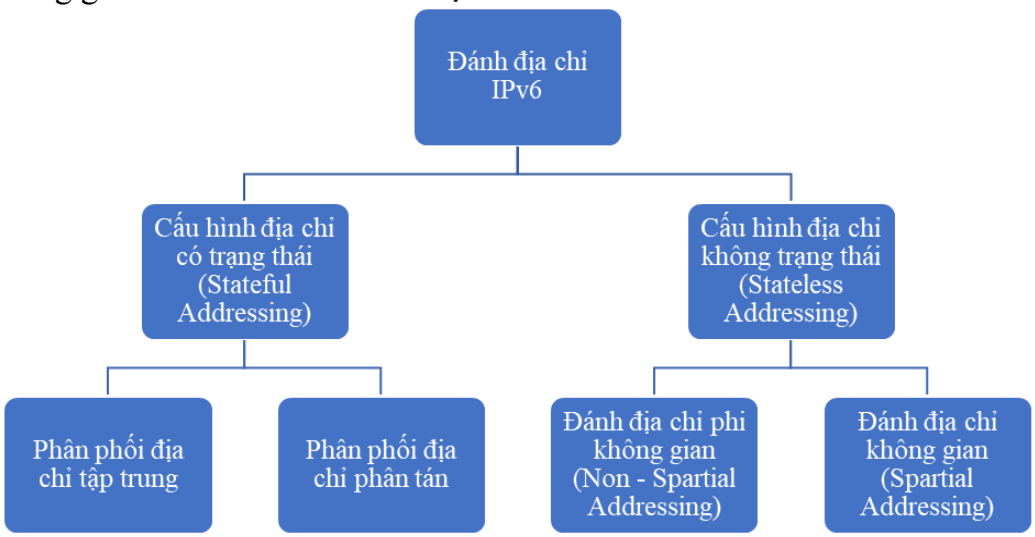
- Gán địa chỉ IPv6 tự động không trạng thái Stateless Addressing (SLAAC): Trong cơ chế này, một tiền tố IPv6 được cấu hình trên giao diện bộ định tuyến và bộ định tuyến quảng bá tới các nút gắn với giao diện. Khi nhận tiền tố tại thời điểm khởi động, nút có thể tự động thiết lập địa chỉ IPv6 của mình. SLAAC được thiết kế để cung cấp cách đơn giản nhất có thể, nhưng năng động cho các nút tự động cấu hình địa chỉ IPv6 cho chính mình. Với SLAAC, nút phải xác định cấu hình địa chỉ liên kết cục bộ cho tất cả các giao diện sử dụng IPv6. Địa chỉ liên kết cục bộ được định hình ngay cả khi không có bộ định tuyến. Các bộ định tuyến trên mạng truyền thông báo ICMPv6 Quảng cáo của Bộ định tuyến (RA) có thể bao gồm các tiền tố IPv6, mà các nút sử dụng để cấu hình một hoặc nhiều địa chỉ ULA hoặc GUA cho nút. Khi một nút nhận được RA, nó sẽ phân tích cú pháp và chọn một hoặc nhiều tiền tố IPv6 64-bit để kết hợp với ID 64-bit đã tạo ra để tạo một hoặc nhiều địa chỉ IPv6 128-bit. SLAAC là cơ chế có khả năng mở rộng cao nhất vì không yêu cầu mạng biết các nút nào tồn tại và địa chỉ nào

chúng đã định cấu hình. Khi các thiết bị tạo địa chỉ của chúng một cách độc lập, để tránh xung đột địa chỉ, giao thức phát hiện địa chỉ trùng lặp (DAD) được sử dụng.

Địa chỉ IPv6 tự động có thể tiếp tục phân thành hai loại dựa trên thông tin được sử dụng để tạo địa chỉ.

+ Spatial Addressing: các địa chỉ được tạo bởi các thuật toán sử dụng thông tin không gian gắn với các thiết bị để tạo địa chỉ.

+ Non-Spatial Addressing: các địa chỉ được tạo bởi các thuật toán sử dụng dữ liệu phi không gian có sẵn trên các thiết bị.



Hình 12 Các cách thức gán địa chỉ IPv6 cho IoT

2.2. Các giải pháp quản lý, phân bổ địa chỉ IPv6 trong IoT

2.2.1. Các nút IoT

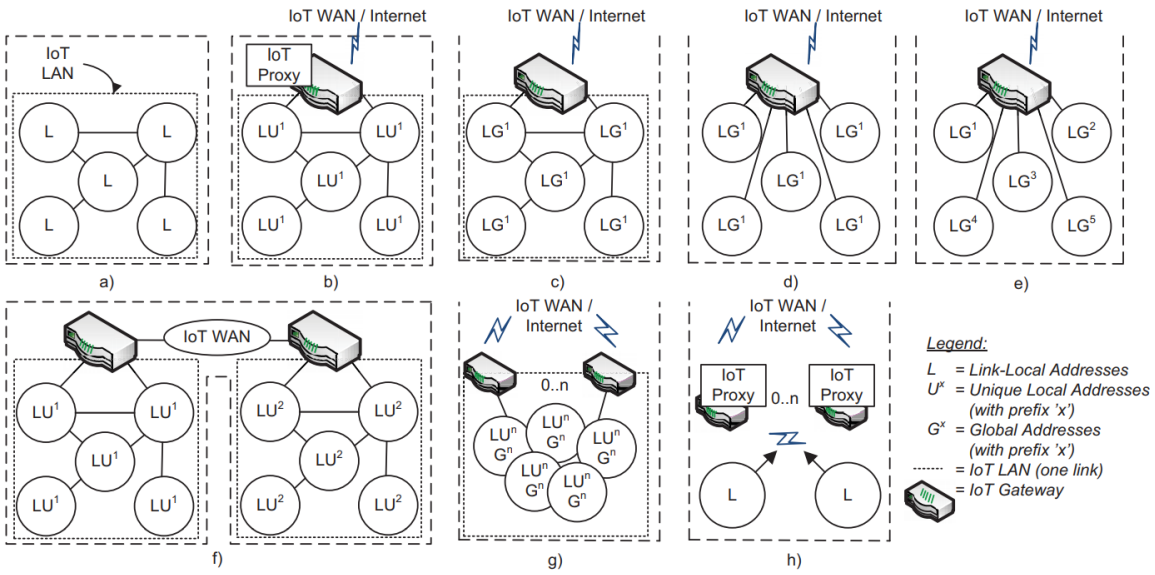
Các cơ chế tương tự được sử dụng để phân bổ địa chỉ của các nút IoT như đối với Internet thông thường — Tự động cấu hình địa chỉ không trạng thái (SLAAC) và Giao thức cấu hình máy chủ động cho IPv6 (DHCPv6). Ngoài ra, các nút có thể được định cấu hình tĩnh (IID) theo nhiều cách khác nhau, bao gồm cả việc dựa trên số nhận dạng phần cứng được mã hóa cứng.

Với các yêu cầu của các mô hình mạng IoT đã mô tả phía trên, cơ chế phù hợp nhất để định địa chỉ nút IoT là SLAAC với địa chỉ ULA hoặc GUA tùy thuộc vào kịch bản triển khai. IID dựa trên phần cứng hoặc được chọn động có thể được sử dụng để tạo địa chỉ liên kết cục bộ, ULA hoặc GUA. Địa chỉ liên kết cục bộ dựa trên định danh phần cứng là lựa chọn xác định địa chỉ duy nhất nếu các nút IoT không có khả năng nhận và do đó không thể thực hiện quy trình Phát hiện địa chỉ trùng lặp.

Cấu hình tĩnh thông qua giao diện quản lý có thể được sử dụng, nhưng chi phí bảo trì hoạt động cao. Do các trường hợp đánh số lại địa chỉ mạng trong IoT, cách thức này là cách tiếp cận không thực tế cho IoT. Mã hóa cứng địa chỉ trong quá trình sản xuất hoặc bằng cách cập nhật lại phần sụn nút IoT, thuộc bất kỳ phạm vi nào khác ngoài liên kết cục bộ không được khuyến khích.

2.2.2. Cổng IoT / Proxy

IoT Gateway và IoT Proxy đóng vai trò các nút trung tâm trong việc phân bổ địa chỉ cho các nút IoT, vì chúng là các bộ định tuyến trong mạng LAN IoT và chịu trách nhiệm cho cả kết nối Internet và có thể là kết nối giữa các mạng LAN IoT. Trong các tình huống C, D, E và G, được minh họa trong Hình dưới đây, cổng quảng bá các tiền tố có thể định tuyến toàn cầu, được sử dụng bởi các nút IoT để cấu hình địa chỉ với SLAAC. Cổng IoT phải lấy tiền tố từ mạng cấp trên với các cơ chế như DHCPv6. Ngoài các tiền tố có thể định tuyến toàn cầu, IoT Gateway hoặc IoT Proxy cũng có thể tạo tiền tố ULA, như được minh họa trong các tình huống B, F và G và quảng bá nó với mạng LAN IoT. Vì các địa chỉ ULA có thể được tạo và duy trì độc lập với các địa chỉ toàn cầu hoặc kết nối Internet, ULA là một lựa chọn tốt để định địa chỉ LAN IoT trong các trường hợp sử dụng mà sự ổn định của địa chỉ nội bộ là quan trọng hoặc yêu cầu kết nối với các LAN IoT khác.



Hình 13 Các mô hình thiết lập mạng LAN IoT

Các nút IoT đơn giản nhất có thể chỉ cung cấp dữ liệu đến Proxy IoT gần nhất, như được minh họa trong kịch bản H trong Hình trên. Trong những trường hợp này, việc sử dụng ULA hoặc GUA có thể là không cần thiết. Các nút đơn giản nhất có thể quản lý bằng địa chỉ liên kết cục bộ (địa chỉ link-local) và sử dụng địa chỉ đa hướng

liên kết cục bộ làm địa chỉ đích của các gói tin. Proxy IoT sẽ thu thập các gói được gửi đến nhóm đa hướng liên kết cục bộ và ủy quyền cho chúng chuyển tiếp.

Khi ULA được sử dụng để cung cấp sự ổn định địa chỉ, nhưng các nút IoT cần giao tiếp với Internet, thì IoT Proxy có thể cần triển khai proxy lớp ứng dụng hoặc có thể Cổng IoT có thể cần hỗ trợ kỹ thuật biên dịch tiền tố (NPTv6). Một proxy lớp ứng dụng cũng có thể thực hiện các xử lý khác, ngoài việc chỉ truyền dữ liệu giữa Internet và các nút IoT.

Cho đến khi Internet chuyển đổi hoàn toàn sang IPv6, cổng IoT có thể chỉ có đường lên IPv4. Do những thách thức trong quá trình chuyển đổi, các triển khai IoT phải được thiết kế để có kết nối thuần IPv6. Nếu không, các giải pháp thay thế tối ưu phải được chọn trong ba phương thức: dịch giao thức từ IPv6 sang IPv4 (ví dụ: NAT64), truyền các gói IPv6 qua IPv4 (ví dụ: 6to4) và chuyển tiếp dữ liệu (ví dụ: proxy lớp ứng dụng).

2.2.3. Kết nối, định tuyến, multihome

- Kết nối mạng phía trên:

Trong một số trường hợp, các cơ chế phân bổ địa chỉ như DHCPv6 có thể không khả dụng. Cổng IoT có thể chỉ được cung cấp một tiền tố duy nhất /64, do vậy nó không thể phân bổ các tiền tố cho mạng LAN IoT. Kịch bản này hiện diện hiện nay, chẳng hạn, trong các mạng 3GPP nơi thiết bị di động được cấp phát một tiền tố /64. Trong trường hợp này, IoT Gateway bằng cách nào đó phải làm "cầu nối" giữa nhà cung cấp cấp trên và IoT LAN.

- Định tuyến:

Trong trường hợp mạng LAN IoT lớn và hoạt động độc lập, việc phân bổ địa chỉ động qua DHCPv6 có thể không cung cấp đủ địa chỉ và đủ khả năng mở rộng. Như với bất kỳ mạng tương đối lớn nào, giao diện giữa IoT LAN và mạng cấp trên hoặc các mạng của nó có thể được thực hiện bằng định tuyến. Khi mạng LAN IoT có không gian địa chỉ từ nhà cung cấp dịch vụ kết nối mạng, các giao thức định tuyến bên trong như OSPF và IS-IS có thể sử dụng. Trong cấu trúc liên kết nơi có nhiều phân đoạn và bộ định tuyến trong IoT WAN, IoT LAN cũng có thể sử dụng giao thức định tuyến để cập nhật vị trí.

- Multihoming:

Cả mạng và các nút IoT đều có thể là multihome. Đối với các mạng nhỏ, chẳng hạn như mạng LAN IoT gia đình, không có không gian địa chỉ riêng, mạng LAN IoT

multihome sẽ có các tiền tố khác nhau từ các kết nối Internet khác nhau. Các cách tiếp cận khác nhau cho vấn đề như sau:

(1) Phương pháp tiếp cận dựa trên proxy

Một proxy quản lý nhiều kết nối cấp trên bằng địa chỉ IP tương ứng của chúng hoặc có các proxy IoT riêng biệt cho mỗi kết nối cấp trên. Ngoài các proxy khác nhau, có thể sử dụng Cổng IoT cung cấp tiền tố từ liên kết cấp trên.

(2) Cổng IoT riêng biệt

Nhiều Cổng kết nối IoT cung cấp không gian địa chỉ của riêng chúng cho Mạng LAN IoT và các Nút IoT multihome. Kịch bản đầu tiên ở trên tương đối đơn giản vì các nút sẽ không nhận thức được multihome. Tuy nhiên, có thể có những trường hợp cách tiếp cận đó quá hạn chế khi giao tiếp giữa nút và mạng cấp trên bị proxy cô lập.

Thách thức của multihome là nút multihome phải biết địa chỉ nguồn nào để sử dụng trong giao tiếp tùy thuộc vào điểm đến và các gói có nguồn gốc IoT LAN phải được định tuyến chính xác qua Cổng IoT. Để lựa chọn Cổng IoT cấp trên, các giao thức định tuyến có thể được sử dụng giữa các Cổng. Tuy nhiên, các quy tắc lựa chọn địa chỉ nguồn IPv6 có thể cung cấp kết quả không tối ưu nếu địa chỉ đích và địa chỉ nguồn không bắt nguồn từ cùng một tiền tố. Nút đa hướng phải sử dụng thông tin chính sách để chọn chính xác địa chỉ nguồn. IETF đã làm việc về các giải pháp đa hướng, ví dụ các chuyên đề của Nhóm làm việc về đa giao diện (MIF).

Nói chung, tính không đồng nhất của thiết bị, mạng IP tương tác với mạng không phải IP và số lượng các thực thể được kết nối, duy nhất đang xác định các tính năng của IoT. Các sơ đồ cấu hình được sử dụng để đánh số các nút IoT phần lớn tương tự như các phương pháp hiện tại để đánh số các nút tiêu chuẩn. Tuy nhiên, thiết bị IoT càng bị hạn chế thì càng có nhiều thách thức xuất hiện và xuất hiện nhiều lĩnh vực cần cải thiện. Đối với các nút IoT bị hạn chế, các sự kiện di động, đa điểm và nói chung là đánh số lại tiêu tốn tài nguyên do nhu cầu giám sát chuyển động và làm mới địa chỉ ngày càng tăng. Tính di động với sự trợ giúp của các điểm neo từ xa đòi hỏi nhiều cơ sở hạ tầng hơn, tính di động dựa trên định tuyến đặt ra các vấn đề về khả năng mở rộng và nếu các sự kiện di động này bị ẩn khi sử dụng ULA, thì các cổng IoT bắt buộc phải triển khai các chức năng trung gian không trong suốt. Các yêu cầu tương tự cũng nảy sinh từ các nút IoT hoạt động ở chế độ một chiều và không thể định cấu hình các địa chỉ phạm vi toàn cầu cho chính chúng. Tất các các vấn đề này cần tiếp tục được giải quyết bằng các nghiên cứu và giải pháp hiệu quả để phục vụ việc gắn địa chỉ IPv6 phạm vi toàn cầu cho mạng IoT.

2.3. Hướng dẫn phân hoạch, cấp phát địa chỉ IPv6 cho IoT

2.3.1 Nguyên tắc phân hoạch

- Phân chia dải địa chỉ ở các mức prefix cố định /32, /40, /48, /56, /64, /128 để dễ quản lí.

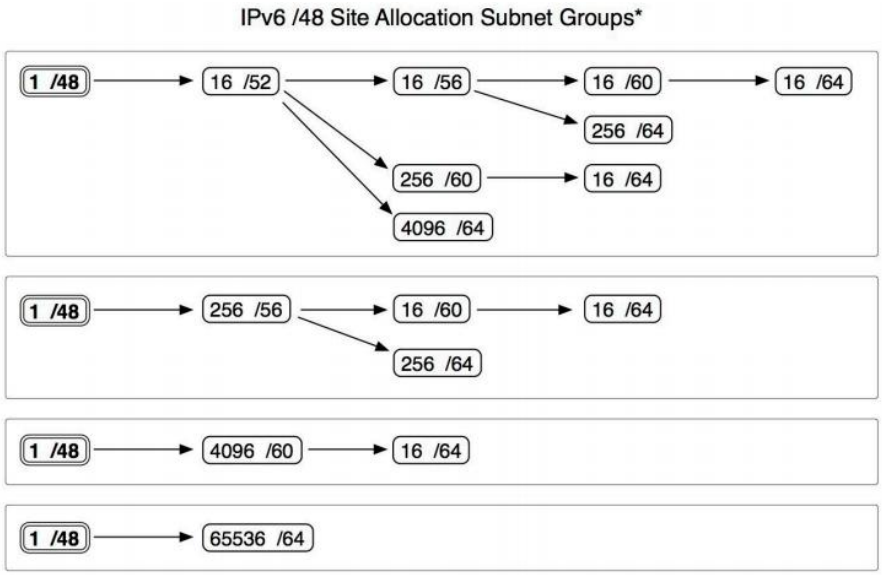
- Tránh sử dụng các chữ cái hệ hexa (A,B,C,D,E,F) cho các địa chỉ hạ tầng (infrastructure addresses), trừ khi đã sử dụng hết các chữ số.

- Qui hoạch dải địa chỉ hạ tầng vào trong 1 single block để sau này dễ sử dụng và quản lí ACL.

- Các địa chỉ Loopbacks, Management, Internal nên qui hoạch trong 1 block /41, trong khi địa chỉ Public qui hoạch trong /41 còn lại.

- Với mỗi PoP, qui hoạch các địa chỉ của khách hàng trong cùng 1 single block để dễ tổng hợp tuyến (route aggregation).

Hình sau minh họa quá trình phân chia block /48 thành các subnet theo prefix có boundary 4 bít:



Hình 14 Phân hoạch các vùng địa chỉ

Phân chia địa chỉ IPv6

Trước tiên, phân loại các PoP (Các điểm truy nhập mạng) của ISP thành 3 mức, tùy theo số lượng khách hàng và nhu cầu sử dụng địa chỉ của PoP đó:

- PoP Level-1 (PoP cỡ lớn).
- PoP Level-2 (PoP cỡ trung bình).
- PoP Level-3 (PoP cỡ nhỏ).

Sau đó, phân loại khách hàng thành 2 loại: Khách hàng cá nhân; Khách hàng doanh nghiệp, tổ chức.

Hiện nay, mỗi ISP được phân chia ít nhất một không gian địa chỉ Ipv6 /32. Từ không gian địa chỉ /32 ban đầu, các ISP phân chia thành các block /40, sau đó phân chia tiếp thành các block nhỏ hơn /48,/56,/64…

2.3.2. Phân hoạch địa chỉ IPv6 cho mạng con

Phân hoạch đánh địa chỉ mạng con phải tính đến các yêu cầu sau:

- Khả năng mở rộng: Số lượng thiết bị được kết nối IoT dự kiến sẽ tăng lên đáng kể với hàng chục tỷ thiết bị giao tiếp. Do đó, một công ty duy nhất hoặc một đơn vị hành chính có thể nhanh chóng tiếp cận vài chục nghìn thiết bị IoT.

- Tương thích tương lai: Các thiết bị và công nghệ IoT mới dự kiến sẽ xuất hiện theo thời gian, cần các mạng con mới.

- Khả năng quản lý: Số lượng thiết bị được kết nối IoT ngày càng tăng sẽ yêu cầu sử dụng các mạng con hợp lý và có cấu trúc tốt để đơn giản hóa việc bảo trì và kiểm soát mạng IoT.

Hơn nữa, trong giai đoạn chuyển đổi từ IPv4 và IPv6, địa chỉ mạng con IPv6 cần đảm bảo cho phép sự cùng tồn tại của các kế hoạch địa chỉ nhất quán giữa IPv4 và IPv6 càng nhiều càng tốt.

Lập quy hoạch, triển khai và cấu hình một kế hoạch đánh địa chỉ tiêu tốn tài nguyên. Tài liệu tham khảo của ITU đề xuất một mô hình linh hoạt và có thể điều chỉnh cho phù hợp với nhu cầu của người dùng cuối, đồng thời cho phép họ hưởng lợi từ mô hình tối ưu hóa để đón đầu sự phát triển của Internet of Things. Một mô hình như vậy sẽ tiết kiệm thời gian và chi phí cho người dùng cuối bằng cách:

- Nới lỏng cấu trúc của các kế hoạch giải quyết mạng con;

- Cho phép người dùng cuối áp dụng quá trình chuyển đổi suôn sẻ từ dual-stack IPv4/IPv6 sang môi trường thuần IPv6;

- Hưởng lợi từ một kế hoạch địa chỉ dự kiến sự mở rộng của Internet of Things.

Phương pháp phân hoạch địa chỉ IPv6 cho mạng con

Với một tiền tố /48 được phân bổ, ID mạng con dài 16 bit, tương ứng có thể cố 65.536 ID mạng con. Để cho phép ánh xạ nhất quán giữa địa chỉ mạng con IPv4 và IPv6, một kế hoạch đánh địa chỉ được đề xuất, với một phần của kế hoạch đánh địa chỉ mạng con IPv6 được thiết kế để lập bản đồ tương ứng. Mô hình tham chiếu cho kế hoạch đánh địa chỉ mạng con IPv6 được cấu trúc như sau:

- Một chữ số thập lục phân đầu tiên (A), tương đương với 4 bit, được sử dụng để xác định các tòa nhà và địa điểm. Nó có thể xác định lên đến 16 vị trí riêng biệt. Một hoặc một số chữ số thập lục phân cũng có thể được dành riêng cho mạng con không được liên kết với bất kỳ tòa nhà hoặc vị trí cụ thể nào để dự phòng.

- Một chữ số thập lục phân thứ hai (B), tương đương với 4 bit, được sử dụng để phân loại các mạng con giữa các thể loại:

+ Danh mục khu DMZ: được sử dụng cho các máy chủ công cộng cho phân đoạn của mạng kết nối trực tiếp với Internet và các tương tác bên ngoài;

+ Loại máy chủ nội bộ: dành riêng cho các máy chủ nội bộ, sao lưu và dung lượng lưu trữ;

+ Danh mục mạng cục bộ (LAN) thông thường;

+ Danh mục Internet of things;

+ Danh mục khác: dành riêng cho bất kỳ phân bổ cụ thể nào khác và cũng có thể được sử dụng để mở rộng một trong các danh mục trước đó. Ví dụ, nó có thể được sử dụng để mở rộng danh mục cho 50% mạng con IoT

- Chữ số thập lục phân thứ ba (C) và thứ tư (D), tương đương với 4 bit mỗi chữ số, được sử dụng để chỉ định mạng con. Tuy nhiên, do yêu cầu ánh xạ địa chỉ IPv4 với IPv6, các chữ số thập lục phân và thứ tư được đặt thành 0, như được chỉ ra trong Hình dưới.

	A	B	C	D
Dual IPv6 - IPv4	0	Category	Subnet	0
Pure IPv6	Prefix	Category	Subnet	Subnet

Hình 15 Cấu trúc đánh subnet

Mô hình được đề xuất cho phép ánh xạ trực tiếp giữa địa chỉ IPv4 và IPv6; tạo điều kiện chuyển đổi từ IPv4 sang IPv6 và đơn giản hóa việc cùng tồn tại của các gói địa chỉ IPv6 và IPv4; tạo điều kiện thuận lợi cho việc chuyển đổi sang mạng IPv6-only.

Hình dưới đây là một ví dụ về mô hình tham chiếu cho kế hoạch định địa chỉ ID mạng con IPv6 đã được chia sẻ với sự hỗ trợ của Viện Kỹ sư Điện và Điện tử -IEEE. Mô hình được đề xuất xác định một kế hoạch giải quyết hai giai đoạn:

1. Kế hoạch định địa chỉ IPv6-IPv4 kép, với ánh xạ hoàn hảo của địa chỉ IPv6 sang địa chỉ IPv4, cho phép chuyển đổi suôn sẻ từ IPv4 sang IPv6 với một kế hoạch định địa chỉ nhất quán.

2. Kế hoạch địa chỉ chỉ IPv6, với khả năng mở rộng kế hoạch địa chỉ theo hướng số lượng nút cuối lớn hơn.

Các kỹ sư mạng cũng có thể kết hợp các kế hoạch định địa chỉ, bằng cách đặt trước các địa chỉ IPv6 được sử dụng trong gói IPv6-IPv4 kép (A) cho kế thừa trong giai đoạn chuyển đổi và trong giai đoạn thứ hai bằng cách sử dụng và phân bổ các địa chỉ IPv6 bổ sung có sẵn trong kế hoạch định địa chỉ IPv6 cho các thiết bị và tài nguyên IPv6 mới được kích hoạt.

	Dual IPv6 - IPv4						Pure IPv6				
	IPv6				IPv4		IPv6				
Allocation	A	B	C	D	octet	Nb	A	B	C	D	Nb
DMZ	0	**0**	0-f	0	0 - 15	32	0-f	**0**	0-f	0-f	16 x 8'192
	0	**1**	0-f	0	16 - 31		0-f	**1**	0-f	0-f	
Internal Servers	0	**2**	0-f	0	32 - 47	32	0-f	**2**	0-f	0-f	16 x 8'192
	0	**3**	0-f	0	48 - 63		0-f	**3**	0-f	0-f	
Regular LAN	0	**4**	0-f	0	64 - 79	64	0-f	**4**	0-f	0-f	16 x 16'384
	0	**5**	0-f	0	80 - 95		0-f	**5**	0-f	0-f	
	0	**6**	0-f	0	96 - 111		0-f	**6**	0-f	0-f	
	0	**7**	0-f	0	112 - 127		0-f	**7**	0-f	0-f	
IoT & Building Automation	0	**8**	0-f	0	128 - 143	64	0-f	**8**	0-f	0-f	16 x 16'384
	0	**9**	0-f	0	144 - 159		0-f	**9**	0-f	0-f	
	0	**a**	0-f	0	160 - 175		0-f	**a**	0-f	0-f	
	0	**b**	0-f	0	176 - 191		0-f	**b**	0-f	0-f	
Others	0	**c**	0-f	0	192 - 207	64	0-f	**c**	0-f	0-f	16 x 16'384
	0	**d**	0-f	0	208 - 223		0-f	**d**	0-f	0-f	
	0	**e**	0-f	0	224 - 239		0-f	**e**	0-f	0-f	
	0	**f**	0-f	0	240 - 255		0-f	**f**	0-f	0-f	

Bảng 2: Phân hoạch vùng IPv6 có liên kết tới IPv4

Kế hoạch địa chỉ nêu trên giải quyết được một số thuộc tính:

- Kế hoạch định địa chỉ cho phép ánh xạ trực tiếp và đơn giản các địa chỉ IPv6 trên các địa chỉ IPv4;

- Phân đoạn được chỉ định cho phép sử dụng các cơ chế lọc dựa trên bit để nhất quán phân biệt các địa chỉ IPv6 theo phân bổ danh mục mạng con của chúng;

- Một phần tư kế hoạch địa chỉ được dành riêng cho các mạng con khác hoặc để mở rộng một trong các các danh mục mạng con trước đó. Ví dụ, điều này cho phép phân bổ lên đến một nửa số địa chỉ đến các thiết bị IoT cho các thực thể có triển khai IoT lớn và lên đến một nửa số địa chỉ vào mạng LAN thông thường cho các thực thể có triển khai IoT có thể dự đoán còn hạn chế;

- Kế hoạch giải quyết được đề xuất cho phép tạo và quản lý tới 65.536 mạng con, bao gồm 32.768 mạng con cho IoT. Sau đó, mỗi mạng con IoT có thể xử lý tới 16 tỷ trong số hàng tỷ nút cuối duy nhất và ID máy chủ duy nhất. Con số này lớn hơn nhiều so với toàn bộ Internet với mỗi và mọi máy chủ trên trái đất. Năng lực này dự kiến sẽ đủ lớn để đáp ứng các ngành công nghiệp và các yêu cầu của cơ quan hành chính nhà nước. Đối với các thực thể yêu cầu số lượng mạng con lớn hơn, vẫn có khả năng mở rộng tiền tố định tuyến toàn cầu để mở rộng đáng kể số lượng mạng con.

- Mô hình được đề xuất có lợi thế là cho phép người dùng tận dụng tối đa IPv4 của họ giải quyết giai đoạn triển khai dual-stack, đồng thời hưởng lợi từ việc định địa chỉ IPv6 đầy đủ tiềm năng cho các thiết bị và nút có thể tạo ra từ IPv4.

- Kế hoạch địa chỉ được đề xuất cho phép quản trị viên mạng dễ dàng phân bổ địa chỉ theo cách có cấu trúc và để xác định và quản lý các nút cuối cho phù hợp. Cấu trúc như vậy cũng giảm bớt quản lý an ninh mạng bằng cách cho phép cấu hình các quy tắc tường lửa khác nhau theo địa chỉ IPv6.

- Kế hoạch giải quyết được mô tả ở trên có thể được tùy chỉnh theo nhu cầu và các yêu cầu cụ thể. Các phạm vi địa chỉ được phân bổ cho từng loại mạng con có thể được điều chỉnh phù hợp.

Chi tiết mô hình tham chiếu cho một số mức tiền tố định tuyến, tham khảo tại Phụ lục 1.

2.3.3. Hướng dẫn cấp phát, gán địa chỉ IPv6 cho IoT

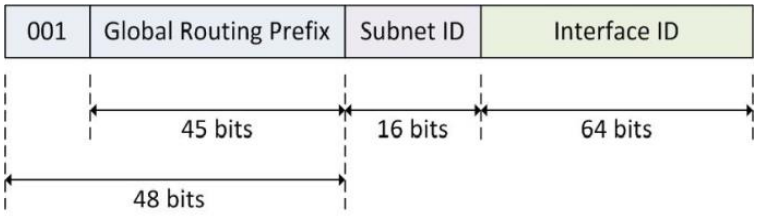
Địa chỉ IPv6 cho chiều dài 128 bit nhị phân; được chia thành 2 phần “network” và “host”. Chi tiết hơn, 64 bit phần “network” được phân chia thành global routing prefix (tiền tố định tuyến toàn cầu) và subnet ID.

3 bit đầu tiên của địa chỉ có thể định tuyến toàn cầu được thiết lập bằng 001.

45 bit tiếp theo định nghĩa vùng địa tuyến toàn cầu (global routing prefix).

16 bit tiếp theo dành cho đánh số mạng con (subnet ID).

64 bit còn lại dành để định danh giao diện (interface ID).



Hình 16 Định dạng địa chỉ unicast toàn cầu IPv6

2.3.3.1. Cấp phát địa chỉ IPv6 cho một hệ thống mạng

Muốn cấp phát địa chỉ IPv6 cho 1 một hệ thống mạng (01 site), trước tiên cần xác định được kích cỡ của site đó. Các tổ chức có 1 site đơn thường được cấp phát một block địa chỉ /48, các tổ chức có nhiều site sẽ được cấp không gian địa chỉ lớn hơn, dựa trên tổng số sites cần đánh địa chỉ. Bảng sau chỉ ra số lượng block /48 có thể hỗ trợ tùy theo số lượng bit của global routing prefix:

Số site /48	Số bít trong phần định tuyến toàn cầu
65.536	32
4.096	36
256	40
16	44
1	48

Bảng 3: Phân hoạch địa chỉ IPv6 cho site

2.3.3.2. Cấp phát địa chỉ IPv6 cho các phân mạng quản lý, dịch vụ

Như phần trên đã đề cập, 1 site thường được cấp 1 block /48. Tiếp theo, các bit Subnet ID trong phần prefix sẽ cho phép phân chia block /48 thành các mạng con (subnet) bên trong 1 site. Tuy nhiên, mọi subnet đều không được nhỏ hơn /64 (định danh giao diện). Bảng sau chỉ ra số lượng subnet mà mỗi block /64 có thể chia nhỏ được tùy theo số bit trong Subnet ID:

Số bít phần định danh mạng con (Subnet ID)	Số mạng con trong /48	Số mạng con /64
48	1	65.536
52	16	4.096
56	256	256
60	4.096	16

Bảng 4: Phân hoạch IPv6 bên trong một site

Bảng trên sẽ giúp xác định với 1 site cho trước cần bao nhiêu nhóm subnet và số block /64 của mỗi subnet. Nhìn chung, mỗi site thường cần các block /64 dành cho các mạng LAN và 1 vài block lớn hơn dành cho các chức năng cụ thể. Một khuyến nghị được đưa ra là khi chia subnet, các prefix nên có boundary là 4 bit một (/48, /52, /56, /60. /64). Điều này giúp dễ quản lí, tổng hợp các subnet đồng thời tạo ra khoảng dự phòng đủ lớn giữa các subnet đáp ứng nhu cầu phát triển của mạng sau này.

2.3.3.3. Hướng dẫn gán tự động địa chỉ IPv6

Cấu hình tự động IPv6 không trạng thái là giải pháp cho gán địa chỉ IPv6 trong IoT. Gán tự động không trạng thái là phương pháp mà các nút IoT trong mạng IPv6 hoặc 6LoWPAN tự động tạo địa chỉ IPv6 của riêng nó. Tự động cấu hình không trạng thái có thể được phân thành hai loại.

+ Gán địa chỉ phi không gian (Non-Spatial Addressing Schemes)

Lược đồ đánh địa chỉ phi không gian không xem xét thông tin không gian của các nút khi tạo địa chỉ. Dưới đây là một số phương pháp xử lý phi không gian đã được nghiên cứu và thiết kế:

(1) EUI-64

Địa chỉ IPv6 duy nhất trên toàn cầu được tạo từ mã nhận dạng duy nhất trên toàn cầu của giao diện mạng, chẳng hạn như dưới dạng địa chỉ MAC 48-bit. Tiền tố cục bộ 64 bit cuối cùng được tạo bởi sử dụng địa chỉ MAC 48 bit. Địa chỉ tổng thể IPv6 được tạo bằng tiền tố quảng bá bởi router và 64 bít định danh giao diện đã tạo từ địa chỉ MAC. Nếu không có tiền tố quảng bá bởi router, các phương pháp khác được sử dụng để tạo địa chỉ IPv6.

(2) Địa chỉ riêng (privacy addtess)

Địa chỉ IPv6 được tạo bằng thuật toán giả ngẫu nhiên, nếu không có sẵn địa chỉ duy nhất toàn cầu hoặc nếu máy chủ muốn cải thiện quyền riêng tư và đảm bảo không thể theo dõi dựa trên IP. Trong lược đồ này, một bản MD5 có giá trị ngẫu nhiên hoặc lưu lịch sử giá trị trước đó được sử dụng để tạo 64 bit cuối cùng của địa chỉ IPv6.

(3) Địa chỉ được tạo bằng mật mã

Để bảo mật các thủ tục IPv6 Neighbor Discovery, địa chỉ IPv6 có thể được tạo từ khóa công khai và được ký bằng khóa riêng. Cách thức này hiếm khi được sử dụng

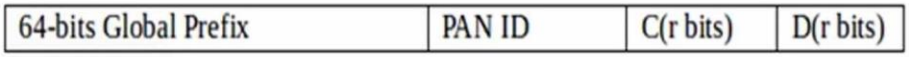
+ Gán địa chỉ không gian (Spatial Addressing Schemes)

Trong lược đồ địa chỉ không gian, các nút sử dụng thông tin vị trí không gian của nó để tạo địa chỉ IP. Dưới đây là một số phương pháp:

(1) Spatial IP Address Assignment - SIPA

SIPA giả định rằng mỗi nút IoT đều biết vị trí không gian của mình và tạo địa chỉ IP của nó một cách độc lập bằng cách lấy tọa độ (x; y) của nút làm hai octet cuối trong địa chỉ IPv4 và 64 bit cuối trong địa chỉ IPv6. Phương pháp SIPA được thực hiện thành công trong Hệ điều hành IoT Contiki (Contiki). Cấu trúc địa chỉ IPv6 được sử dụng trong SIPA như hình dưới đây, trong đó C và D được tính bằng công thức :

C = [x*(2r -1)/Max(x)] và D = [y*(2r -1)/Max(y)]



Hình 17 Cấu trúc địa chỉ SIPA

SIPA dễ triển khai nhưng tỷ lệ thành công trong gán địa chỉ (Address Success Rate ASR) của nó không bao giờ đạt 50% khi số nút nhiều hơn 300 khi r = 8 bit.

- Ưu điểm: (1) SIPA lấy tọa độ (X, Y) của nút để tạo ra các bit cuối của địa chỉ IP. (2) SIPA tận dụng mối quan hệ giữa các vị trí không gian trong việc định tuyến, và không cần máy chủ trung tâm cũng như giao tiếp giữa các nút để tạo địa chỉ IP.

- Nhược điểm: (1) Trong cơ chế này, không có gì đảm bảo rằng mỗi nút sẽ có địa chỉ duy nhất vì hai hoặc nhiều nút liền kề có thể tạo ra cùng một địa chỉ IP. (2) Sự thành công tỷ lệ SIPA không bao giờ có thể là 100% với nhiều hơn một nút.

(2). Chỉ định IP dòng quét (Scan-line IP Assignment - SLIPA)

Chỉ định IP dòng quét (SLIPA) là một phương pháp theo đó chỉ định mọi nút với địa chỉ duy nhất của riêng nó. Phương pháp SLIPA quét mọi nút có cùng giá trị tọa độ Y nhỏ nhất từ trái sang phải và sau đó quét các nút với giá trị tọa độ Y thành công và lặp lại quy trình cho đến khi tất cả các nút đã được quét. Nếu tìm thấy hai hoặc nhiều nút liền kề tạo cùng một địa chỉ IP, SLIPA sẽ "di chuyển lên" các nút liền kề để đảm bảo một địa chỉ chỉ thuộc về một nút mà không làm hỏng mối quan hệ không gian giữa các nút. Nếu hai hoặc nhiều nút được gán cho cùng một IP địa chỉ, thì việc gán địa chỉ không không thành công. Thử nghiệm cho thấy SLIPA có hiệu suất tốt hơn đối với số lượng nút tối đa có thể gắn địa chỉ thành công theo các mô hình bố trí khác nhau của nút. Cấu trúc địa chỉ SLIPA giống như mô tả cấu trúc của SIPA nhưng các tham số C và D được xác định bằng hương trình như sau:

Q = [max(x)-min(x)]/(2r - 1)

C = [{(x-min(x)}/Q]

D được tính toán dựa trên việc sắp xếp các nút theo tọa độ Y và gán số thứ tự dòng cho các nút có cùng giá trị.

D = D(k, SN) = SN nếu k = 1,

D = D(k, SN) = D(k-1, SN) + 1 nếu k > 1

Trong đó SN là số dòng quét bắt đầu từ 0 và k biểu thị nút thứ k có cùng tọa độ Y giá trị. Kết quả mô phỏng cho thấy tỉ lệ thành công trong gán địa chỉ của SLIPA là 100% khi số lượng nút trong mạng từ 700 đến 1250 nếu r = 8bit.

- Ưu điểm: (1) Thuật toán SLIPA cải thiện tỷ lệ gán địa chỉ thành công, cao hơn SIPA. (2) SLIPA có thể đạt được ASR tốt khi các nút được phân bố đều đặn.

- Nhược điểm: (1) Nếu các nút được triển khai theo phân bố ngẫu nhiên, các cải thiện của SLIPA sẽ bị giảm xuống. (2) Dòng quét không thành công khi số dòng đạt đến 2r vì octet cuối cùng trong địa chỉ IP không thể vượt quá 2r -1.

(3) Chỉ định IP dòng quét với phân vùng số lượng bằng nhau (SLIPA-Q)

SLIPA-Q sử dụng phân vùng số lượng bằng nhau thay vì phân vùng khoảng cách bằng nhau của SLIPA. SLIPA-Q dựa trên khái niệm dòng quét và một dạng tối ưu hóa của lược đồ gán địa chỉ IP SLIPA. Cấu trúc địa chỉ IPv6 của SLIPA-Q giống như SLIPA và giá trị của C và D được tính toán dựa trên phương pháp dưới đây:

Q = t/(2r -1) với t là tổng số note trong mạng.

Z = int(i/Q), với là số thứ tự của note được tính theo trục X và bắt đầu từ vị trí 0.

$C = ((i - i^l) \bmod (Z^h - Z^l + 1)) + (Z^h - Z^l + 1)$ nếu Q >= max_node(Z)

$C = ((Z+1) \bmod (Z^h - Z^l + 1)) + (Z^h - Z^l + 1)$ nếu Q< max_node(Z).

i^l chỉ định giá trị thứ tự thấp nhất; Z^h chỉ định giá trị zone cao nhất và Z^l chỉ định giá trị zone thấp nhất.

D = D(k,SN) = SN nếu k = 1

D = D(k,SN) = D(k-1,SN)+1 nếu k > 1

Thử nghiệm cho thấy SLIPA-Q hoạt động tốt hơn SLIPA và SIPA để gán IP với phân bố và số lượng nút khác nhau. Thử nghiệm SLIPA-Q 1.000 lần với 1.000 nút được triển khai ngẫu nhiên; tỷ lệ thành công trong gán địa chỉ trung bình thu được bởi SLIPA-Q cao gấp đôi so với SLIPA. Với cùng tỉ lệ thành công 88%, số lượng nút trung bình mà SLIPA-Q, SLIPA và SIPA có thể gán thành công lần lượt là 950, 850 và 135.

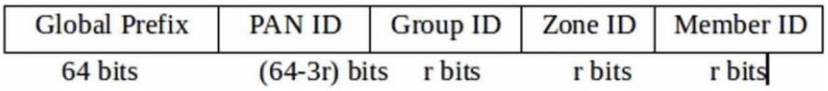
- Ưu điểm: (1) SLIPA-Q thay thế phân vùng khoảng cách bằng nhau bằng phân vùng số lượng bằng nhau và sử dụng tỷ số thành công (ASR) làm chỉ số hiệu suất

chính để thể hiện khả năng gán địa chỉ IP. (2) Lược đồ này duy trì mối quan hệ không gian giữa các nút.

- Nhược điểm: (1) Lược đồ này bị giới hạn trong không gian hai chiều và không đề cập đến cách để đối phó với tính di động của các nút trong mạng. (2) Lược đồ này cũng không đảm bảo tính IP duy nhất.

(4) Gán địa chỉ IP đa chiều (MPIPA)

Khái niệm cơ bản của MPIPA là áp dụng lược đồ chiếu để biểu diễn các nút từ ba chiều không gian thành không gian hai chiều, sau đó áp dụng phân vùng số lượng bằng nhau và lược đồ dòng quét được sử dụng trong SLIPA-Q để tính ID vùng và ID thành viên của mỗi nút theo tọa độ x và tọa độ y của chúng. Trong MPIPA, các nút báo cáo thông tin vị trí ba chiều của chúng cho trạm gốc (BS) để yêu cầu địa chỉ IP sau khi được triển khai trong mạng. BS sẽ thực hiện MPIPA để xác định địa chỉ IP của các nút bằng cách sử dụng thông tin vị trí các nút. Cấu trúc địa chỉ IPv6 của MPIPA được như hình dưới đây. ID vùng và ID thành viên được xác định tương tự như trường SLIPA-Q C và D.



Hình 18 Cấu trúc địa chỉ IPv6 MPIPA

ID nhóm được xác định bằng cách phân chia các tọa độ z thành các nhóm 2r (từ 0 đến 2r -1). MPIPA sử dụng hai loại các phương pháp phân nhóm:

- Phân nhóm dựa trên khoảng cách: Distance Based Grouping (MPIPA-D). G = (max(z)-min(z))/2^r -1; Gid = int ((node(z)-min(z))/G).

- Phân nhóm dựa trên số lượng: Quantity Based Grouping (MPIPA-Q).

G= giá trị thứ tự của note theo chiều hướng Z. Q=t/2^r -1; Gid = int(G/Q)

Kết quả thử nghiệm cho thấy khi r = 9 bit trong SIPA và r = 6 bit trong MPIPA được sử dụng thì tỷ lệ gán địa chỉ thành công của SIPA giảm xuống 0 trong khi MPIPA-D và MPIPA-Q vẫn duy trì 100% với số lượng nút trên 6000. MPIPA-Q có (ASR 90%) hoạt động tốt hơn MPIPA-D (ASR 45%) khi số lượng các nút là khoảng 80.000.

- Ưu điểm: (1) MPIPA mở rộng không gian hai chiều thành không gian ba chiều để gán địa chỉ IP trong mạng. (2) MPIPA cũng có thể được áp dụng trong mạng

dựa trên IPv6 bằng cách xác định ID giao diện ở định dạng địa chỉ IPv6 tiêu chuẩn. (3) MPIPA có thể đạt được ASR cao hơn các phương pháp khác.

- Nhược điểm: (1) MPIPA chỉ có thể được sử dụng khi các nút được cố định. (2) MPIPA không đảm bảo tạo địa chỉ IP duy nhất của các nút.

(5) Chỉ định địa chỉ IP không gian phân tán (DSIPA)

DSIPA là gán một địa chỉ IP cho nút dựa trên khám phá hàng xóm. Trong DSIPA, các nút có địa chỉ IP có trách nhiệm gán địa chỉ IP cho hàng xóm của nó bằng cách sử dụng tọa độ vị trí. Mỗi nút tạo ra địa chỉ IPv6 bằng cách chuyển vị trí thực của chúng vào tọa độ vị trí hợp lý, do đó, mọi nút duy trì mối quan hệ không gian với nhau. Không gian thông tin có thể được sử dụng để thực hiện định tuyến địa lý.

- Ưu điểm: (1) Mối quan hệ giữa các nút có thể được xác định dựa trên địa chỉ IP của chúng. (2) Tiêu thụ năng lượng ít hơn trong quá trình tạo địa chỉ IP.

- Nhược điểm: (1) Địa chỉ trùng lặp có thể được tạo ra. (2) DSIPA chỉ có thể được sử dụng khi các nút được cố định.

Đánh địa chỉ trong IoT là một trong những thách thức lớn nhất trong triển khai IoT. Bảng dưới đây so sánh tất cả các phương thức gán địa chỉ IPv6 không trạng thái phổ biến cho mạng IoT trên cơ sở so sánh các chỉ số quan trọng:

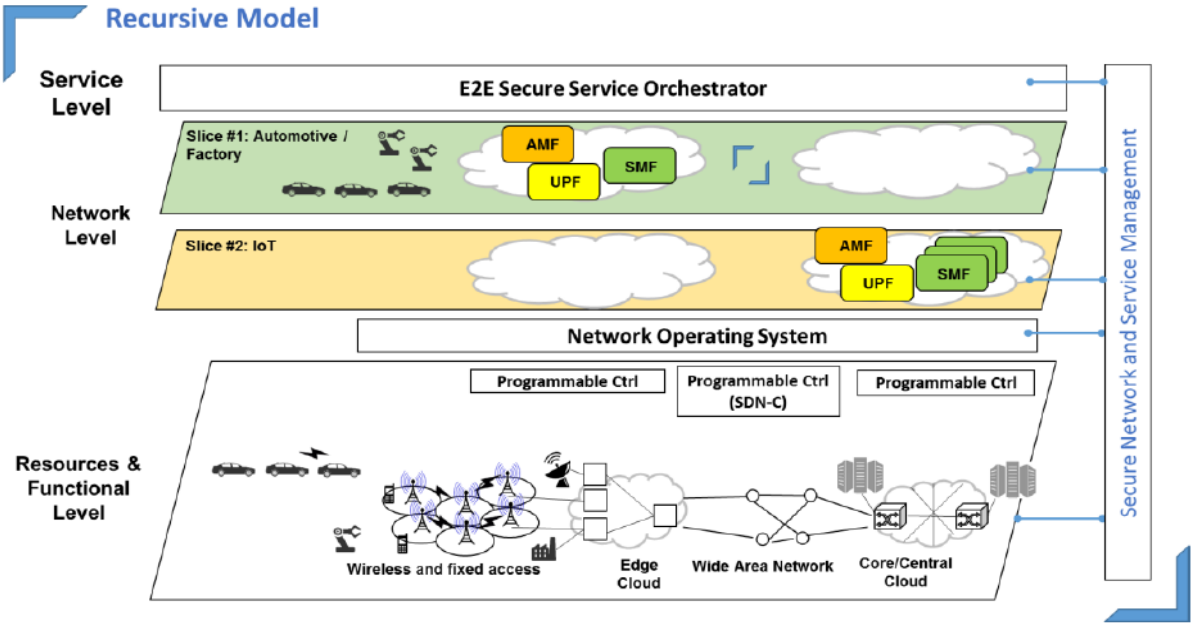
Phương pháp gán địa chỉ	**Thể loại**	**Phạm vi tính duy nhất**	**Tái sử dụng địa chỉ**	**Tiêu thụ năng lượng**	**Quá tải giao tiếp**	**Thông tin vị trí**
EUI- 64	Phi không gian	Có	Không	Thấp	Không	Không
Địa chỉ riêng	Phi không gian	Có	Có	Thấp	Thấp	Không
Địa chỉ mã hóa	Phi không gian	Có	Không	Cao	Cao	Không
SIPA	Không gian	Không	Có	Cao	Cao	Có
SLIPA	Không gian	Không	Có	Cao	Cao	Có
SLIPA-Q	Không gian	Không	Có	Cao	Cao	Có
MPIPA	Không gian	Có	Có	Thấp	Thấp	Có
DSIPA	Không gian	Có	Có	Thấp	Thấp	Có

Bảng 5: Bảng so sánh các phương pháp gán địa chỉ IPv6 trong IoT

PHẦN 3: HƯỚNG DẪN TRIỂN KHAI IPv6 CHO 5G

3.1. Mô hình kiến trúc triển khai IPv6 cho 5G

Mạng 5G là thế hệ mạng mới đáp ứng các yêu cầu cao hơn của một xã hội di động, được kết nối vạn vật. Với sự phát triển của Internet, chuyển đổi số, các ứng dụng được phát triển mạng và lấy con người là trung tâm. Mạng 5G hỗ trợ nhu cầu giao tiếp giữa các ứng dụng, giữa thiết bị với thiết bị, giữa con người với con người. Giúp cuộc sống thuận tiện, an toàn và hiệu quả cao. Kiến trúc mạng 5G được thiết kế để phù hợp với khả năng kết nối nhiều thiết bị, tự động hóa cao.

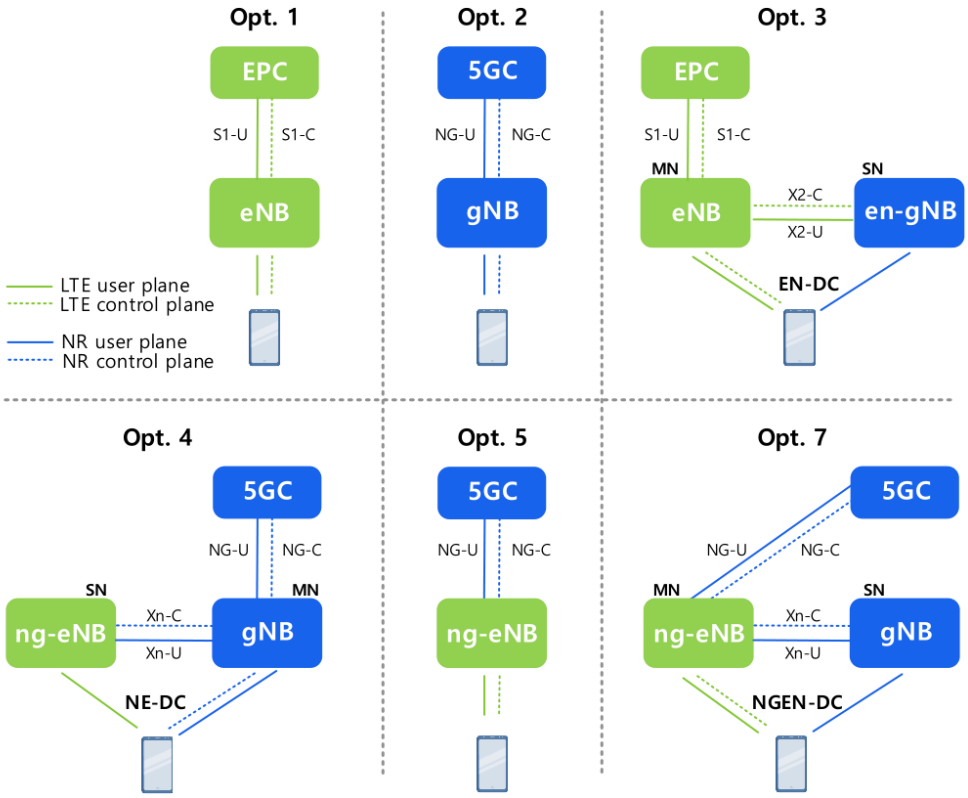


Hình 19 Kiến trúc tổng quan của mạng 5G

Phần lớn các mạng 5G trên thế giới hiện nay đang triển khai theo mô hình "5G phụ thuộc" (5G NSA – Non StandAlone) sử dụng chung hạ tầng mạng truy nhập (Access Network) và mạng lõi (Core Network) sẵn có của mạng 4G. Việc này tận dụng thiết bị cũng như vùng phủ hiện có giúp giảm chi phí, nâng cao hiệu quả đầu tư và rút ngắn thời gian triển khai. Mô hình 5G NSA chỉ mới chỉ giúp cải thiện tốc độ truyền dữ liệu (eMBB-enhanced Mobile Broadband) mà chưa giải quyết được yêu cầu độ trễ cực thấp (urLLC-ultra reliable Low Latency Communications) và đáp ứng số lượng kết nối đồng thời cực lớn trong cùng một phạm vi (mMTC-massive Machine Type Communications). Mô hình 5G NSA chỉ mới là điện thoại di động và máy tính bảng. Vì thế đây không phải là mô hình để hướng đến mục tiêu lâu dài. Mô hình "5G độc lập" (5G SA – StandAlone) được coi là mô hình 5G thực thụ với sự tách bạch hoàn toàn hệ với hệ thống mạng 4G.

Mô hình triển khai 5G và lộ trình chuyển đổi sang mạng 5G SA

Nhóm chuẩn hóa về mạng di động 3GPP đã đưa ra các kịch bản kiến trúc cho mạng 5G như hình dưới, gồm có 7 mô hình chính và được chia thành 2 nhóm kịch bản.



Hình 20 Các kịch bản kiến trúc cho mạng 5G

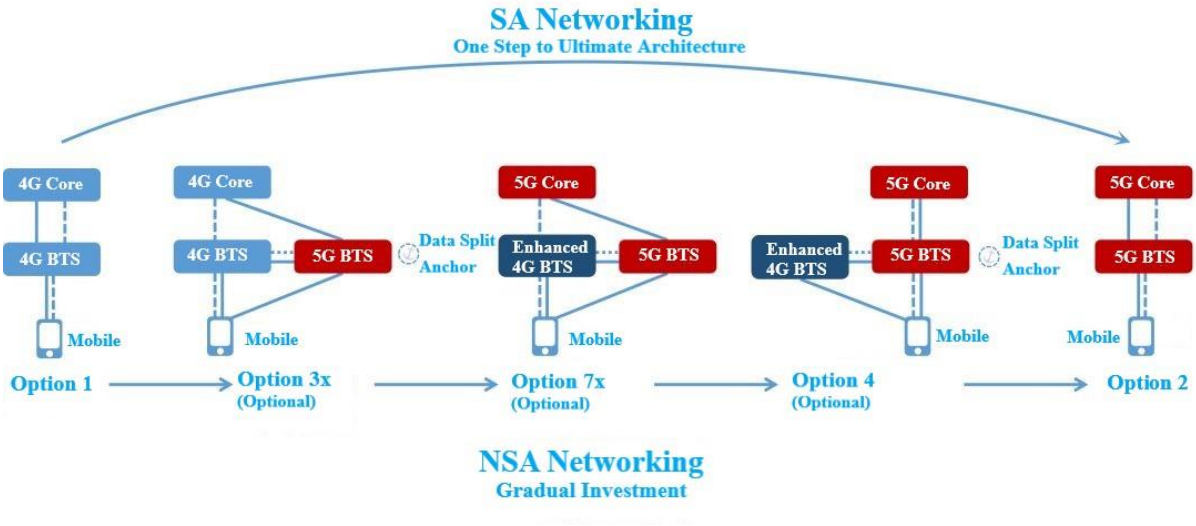
- Nhóm 5G SA gồm các mô hình: 1, 2 và 5
- Nhóm 5G NSA gồm các mô hình: 3, 4 và 7

Thực tế triển khai của các nhà mạng thì mô hình 3 được sử dụng phổ biến nhất nhằm tận dụng hệ thống và vùng phủ hiện tại của mạng 4G. Mô hình 2 là kiến trúc mục tiêu mà các nhà mạng hướng đến để có được mạng 5G thực thụ. Nếu chọn triển khai mô hình 3 thì nhà mạng sẽ cần một thời gian khá dài để chuyển đổi sang mô hình 2 trong tương lai. Các mô hình 4, 5 và 7 được gọi là mô hình bổ sung nhằm kết hợp năng lực của hệ thống Core 5G (5GC) cùng với vùng phủ của 4G. Tuy nhiên mô hình 5 được cho là không mang lại nhiều lợi ích vì không tận sức mạnh của chuẩn vô tuyến 5G NR (New Radio). Trong khi đó mô hình 4 và 7 cho phép kết nối kép (Dual) 4G và 5G, không cần chuyển tiếp (Hand-over) giữa các hệ thống Core hoặc Access của hai mạng. Ngày 25/02/2022, Samsung và SK Telecom tuyên bố đã thử nghiệm thương mại thành công mô hình 4 lần đầu tiên trên thế giới. Đây có thể coi là một phương án phù hợp cho việc xây dựng mạng Core 5G.

Với những mô hình như trên, lộ trình chuyển đổi từ 4G sang mạng 5G SA có thể chia ra thành 02 kịch bản:

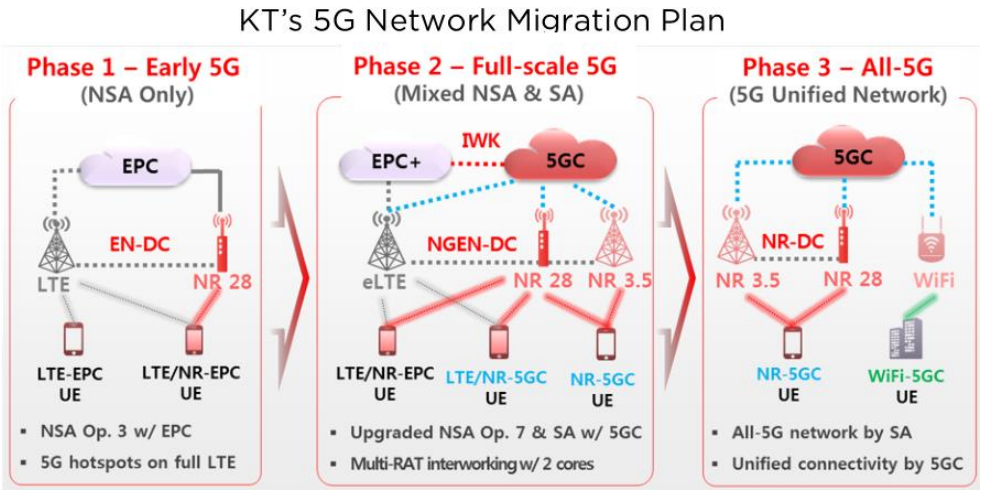
Lộ trình 1: Chuyển đổi trực tiếp sang mô hình 2. Việc này đòi hỏi đầu tư khá lớn từ ban đầu về cả tài lực và nhân lực.

Lộ trình 2: Chuyển đổi trung gian từ mô hình **1 => 3 => 7 => 4 => 2**. Các bước trung gian này là tùy chọn, không nhất thiết thực hiện đầy đủ các bước trung gian.



Hình 21 Lộ trình chuyển đổi trung gia từ mạng 4G sang 5G

Lộ trình 2 trông rất phức tạp và tổng chi phí cũng như thời gian sẽ cao hơn so với đầu tư một lần nhưng việc triển khai sẽ gặp ít rủi ro và việc đầu tư từng giai đoạn phù hợp với nhiều nhà mạng. Dưới đây là lộ trình minh họa cho chiến lược chuyển đổi sang mạng 5G SA của nhà mạng KT của Hàn Quốc.



Hình 22 Mô hình chuyển đổi sang 5G độc lập từ nhà mạng KT Hàn Quốc

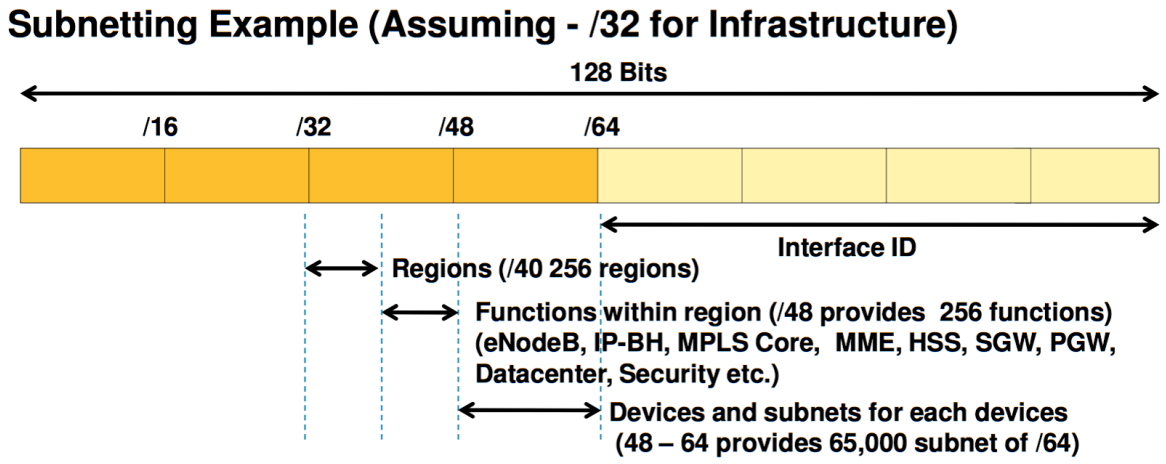
3.2. Hướng dẫn phân hoạch, cấp phát IPv6 cho mạng 5G

3.2.1. Hướng dẫn phân hoạch IPv6 cho 5G

Kiến trúc 5G được xây dựng để hỗ trợ IPv4, IPv6. Điều quan trọng trong phân hoạch, cấp địa chỉ trong mạng 5G đòi hỏi thiết bị đầu cuối khách hàng (CPE) hỗ trợ IPv4/IPv6.

3.2.1.1. Phân hoạch IPv6 cho phần hạ tầng

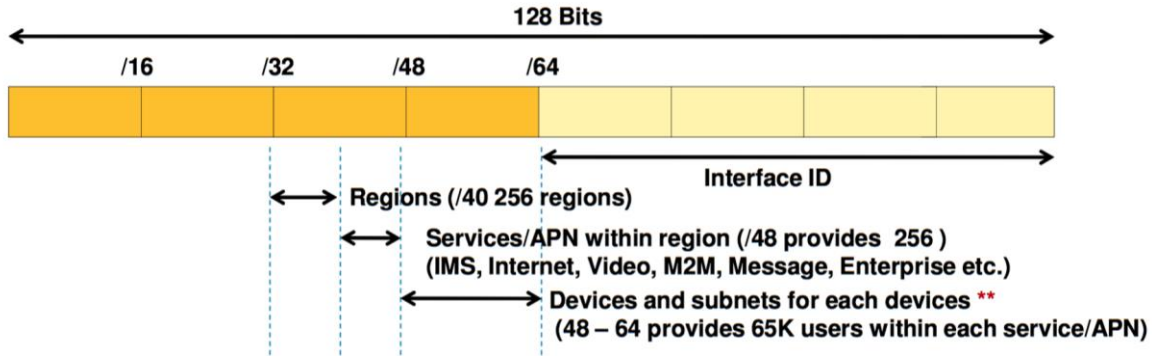
Phân hệ hạ tầng không kết nối Internet sử dụng vùng IPv6: Fc00::/7. Đây là vùng địa chỉ dành riêng cho phân hệ nội bộ, không quảng bá trên Internet toàn cầu.



Hình 23 Phân hoạch IPv6 cho hạ tầng 5G (nguồn: ITU MUST)

3.2.1.2. Phân hoạch IPv6 cho thuê bao

Địa chỉ IPv6 phân hoạch cho thuê bao là địa chỉ global, được cấp, phân bổ cho các tổ chức, doanh nghiệp thông qua các tổ chức quản lý khu vực (RIR), tổ chức quản lý cấp quốc gia (NIR). Tại Việt Nam, địa chỉ IPv6 toàn cầu là địa chỉ được VNNIC cấp, phân bổ.



Hình 24 Phân hoạch IPv6 cho thuê bao 5G (nguồn ITU MUST)

3.2.2. Hướng dẫn cấp địa chỉ IPv6 cho 5G

Cấp IPv6 cho 5G có thể triển khai cấp động hoặc cấp tĩnh địa chỉ. Trường hợp cấp động, hệ thống tự động cấp và gán địa chỉ IP cho thiết bị người dùng (user equipment – UE) 5G. Trường hợp cấp tĩnh, hệ thống cấp IP cố định cho UE.

3.3. Hướng dẫn triển khai công nghệ IPv6-only cho 5G

Hiện nay, công nghệ chuyển đổi IPv6 chủ đạo là công nghệ Dual-stack. Tuy nhiên, giải pháp lâu dài cho 5G, IoT là công nghệ IPv6-only. IPv6-only giúp giải quyết vấn đề hạn chế của IPv4, tối ưu chi phí quản trị. Để triển khai mạng di động 4G, 5G, các nhà mạng trên thế giới đã lựa chọn triển khai IPv6-only và sử dụng giải pháp công nghệ 464XLAT.

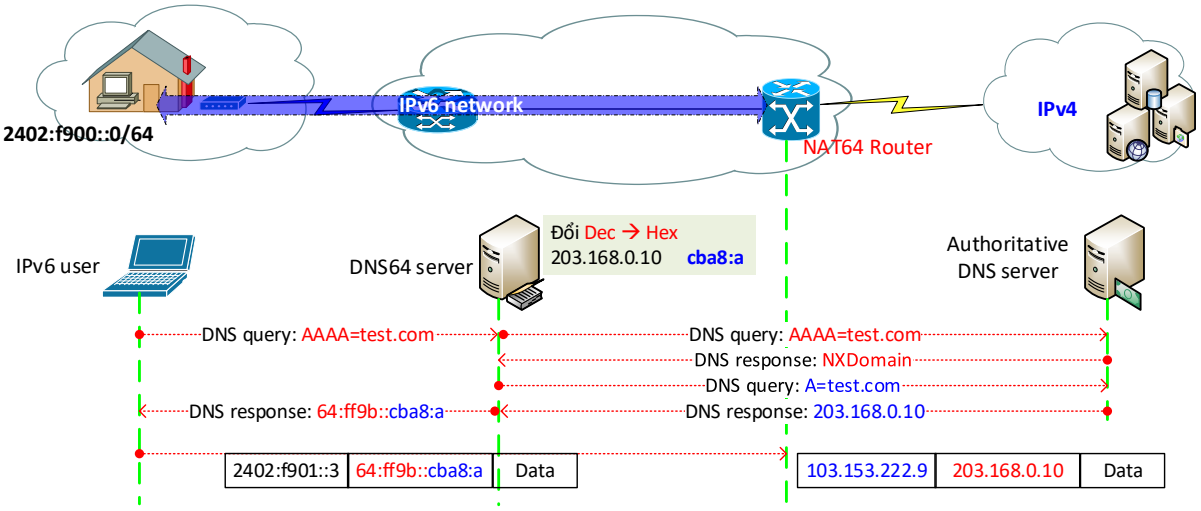
Sau khi chuyển sang IPv6-Only, để một máy trạm có thể kết nối đến một máy đích IPv4-Only bên ngoài thì cần có sự chuyển đổi giữa 2 địa chỉ, vì thế kỹ thuật NAT64 (RFC 6146) đã được đề xuất cùng với sự kết hợp của kỹ thuật DNS64 (RFC 6147). Dưới đây là những thành phần chính và hoạt động của giải pháp kết hợp này:

- **NAT64 prefix**: đây là 1 Prexfix (tiền tố) IPv6 kết hợp địa chỉ IPv4 đích để trở thành địa chỉ đích IPv6 tổng hợp (Synthesized). Nat64 Prefix này có thể được quy định (Well Known Prefix - WKP) là dãy 64:ff9b::/96 hoặc do nhà mạng quy hoạch (Network Specific Prefix – NSP).

- **DNS64 server**: Hoạt động như 1 DNS Server thông thường nhưng nếu truy vấn bản ghi AAAA cho một tên miền không tồn tại thì nó sẽ tiếp tục truy vấn bản tin A. Địa chỉ IPv4 của bản tin A sẽ được chuyển đổi sang dạng HEXA rồi kết hợp với NAT64 Prefix để trở thành địa chỉ IPv6 tổng hợp và sau đó trả về trường AAAA cho máy tính IPv6-Only.

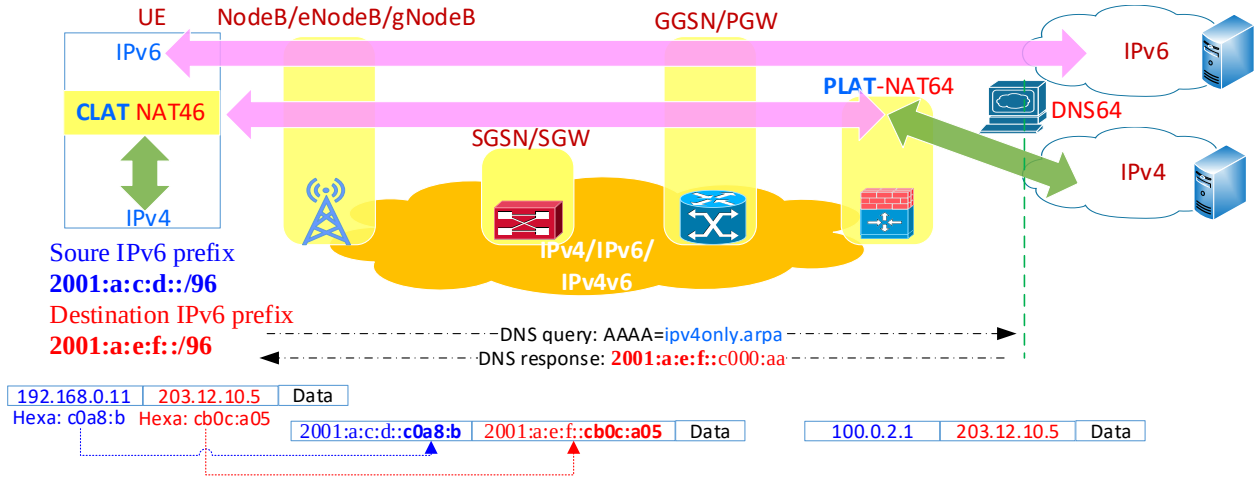
- **NAT64 router:** Router này có nhiệm vụ chuyển đổi IPv6 nguồn thành địa chỉ IPv4 và địa chỉ đích IPv6 tổng hợp thành địa chỉ đích IPv4 ban đầu. Để các gói tin có đích là IPv6 tổng hợp đi đến NAT64 Router thì Router này cần phải quảng bá NAT64 Prefix cho toàn bộ mạng IPv6-Only.

Giải pháp DNS64/NAT64 dù giải quyết được phần lớp các yêu cầu truy cập IPv4 qua môi trường IPv6-Only nhưng vẫn tồn tại trường hợp một số ứng dụng không sử dụng tên miền mà sử dụng địa chỉ IPv4 trong phần IP Payload (gọi là Literal IP). Hoặc nếu một điện thoại di động chuyển sang chế độ phát sóng Wifi (Hot-spot) cho các thiết bị khác (Tethering device) và các thiết bị đó chỉ hỗ trợ IPv4-Only thì không thể truy cập qua mạng IPv6-Only. Có một vấn đề khác cần chú ý đó là DNS64 thực hiện chuyển đổi địa chỉ IP4 thành IPv6 nên nó không thể hoạt động trong trường hợp sử dụng giao thức bảo mật DNSSEC.



Hình 25 Giải pháp chuyển đổi sang thuần IPv6 DNS64/NAT64

Chính vì thế kỹ thuật 464XLAT (RFC 6877) đã ra đời. Kỹ thuật này giải quyết triệt để những vấn đề của giải pháp DNS64/NAT64. Dưới đây là thành phần chức năng và hoạt động của giải pháp 464XLAT.



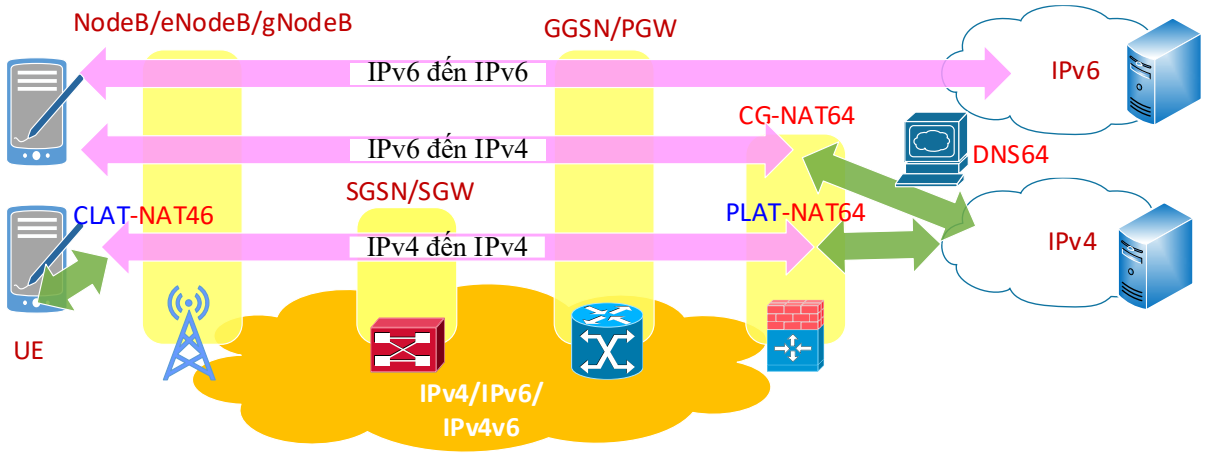
Hình 26 Giải pháp chuyển đổi sang thuần IPv6 464XLAT

- **CLAT** (Customer-side transLATor - RFC6145): Đây là chức năng hoạt động tại thiết bị đầu cuối (UE) như điện thoại di động, có nhiệm vụ chuyển đổi địa chỉ IPv4 nguồn và đích thành IPv6 (NAT46). Thiết bị UE được gán một IPv6 Prefix /64, từ đó lấy ra Prefix /96 (NAT46 Prefix) để kết hợp với địa chỉ IPv4 nguồn để tạo ra địa chỉ nguồn IPv6 tổng hợp. Đối với địa chỉ đích IPv4 thì UE sẽ tự động gửi một truy vấn AAAA có tên "***ipv4only.arpa***" đến DNS64 Server và Server này trả về địa chỉ IPv6 tổng hợp có chứa NAT64 Prefix như trình bày ở giải pháp trước. Sau đó kết hợp với địa chỉ IPv4 đích để tạo ra địa chỉ đích IPv6 tổng hợp. Việc thực hiện ở đây theo kiểu NAT 1:1 nên được gọi là Stateless NAT.

- **PLAT** (Provider-side transLATor - RFC6416): Có nhiệm vụ thực chuyển đổi từ địa chỉ IPv6 tổng hợp (nguồn và đích) sang IPv4 và ngược lại. Để tiết kiệm địa chỉ IPv4 thì việc NAT địa chỉ nguồn được thực hiện theo kiểu N:1 hay còn gọi là Statefull NAT. Router PLAT quảng bá NAT64 Prefix nên các những gói tin có địa chỉ đích IPv6 tổng hợp sẽ đi qua PLAT. PLAT có thể can thiệp được lớp ứng dụng (Application Layer Gateways - ALG) để thay đổi địa chỉ IPv4 nếu có trong IP Payload.

Giải pháp 464XLAT kết hợp DNS64 khá đơn giản và dễ dàng triển khai nên là được các nhà mạng ưu tiên lựa chọn cho mô hình IPv6-Only. Nếu doanh nghiệp cung cấp đồng thời dịch vụ di động và cố định có thể sử dụng chung giải pháp 464XLAT này để tiết kiệm chi phí đầu tư và vận hành. Có một yêu cầu đối với giải pháp 464XLAT đó là thiết bị đầu cuối bắt buộc phải hỗ trợ tính năng CLAT. Đối với điện thoại di động, hệ điều hành Android và Windows đã hỗ trợ tốt tính năng này còn iOS thì không hỗ trợ. Thay vào đó Apple yêu cầu từ ngày 01/6/2016, tất cả các ứng dụng đăng ký lên AppStore phải hỗ trợ IPv6-Only.

Như vậy giải pháp DNS64/NAT64 sẽ hỗ trợ các thiết bị IPv6-Only có thể truy cập được các dịch vụ có đích là IPv4-Only và giải pháp 464XLAT hỗ trợ các ứng dụng sử dụng nguồn và đích là địa chỉ IPv4. Một số nhà mạng triển khai đồng thời cả 2 giải pháp này và được xem như là giải pháp triệt để nhất cho hệ thống mạng IPv6-Only.



Hình 27 Giải pháp chuyển đổi sang thuần IPv6 kết hợp

Trước sự phát triển mạnh mẽ của mạng 5G và IoT thì xu thế chuyển sang mạng thuần IPv6 là điều bắt buộc chứ không còn là một lựa chọn như trước nữa. Đã có những cố gắng mang tính toàn cầu để thúc đẩy việc chuyển đổi này như tháng 11/2016 tiểu ban IETF IAB (Internet Architecture Board) đã ra thông báo sẽ dừng hỗ trợ địa chỉ IPv4 đối với tất cả các tiêu chuẩn hoặc giao thức nghiên cứu mới hoặc mở rộng và tổ chức 3GPP đang cân nhắc bắt buộc sử dụng thuần IPv6 trong mạng 5G độc lập. Ngoài ra như đã trình bày, các quốc gia cũng đang quyết tâm hướng tới mạng thuần IPv6.

Đối với 5G, sau những thành công trong việc thương mại hóa trên thế giới, các giải pháp cho mạng 5G cũng đã chín muồi nên việc chuyển sang giải pháp 5G độc lập ngày càng được lựa chọn hơn. Mạng 5G độc lập sẽ mở ra một kỷ nguyên mới, tạo ra những cơ hội mới và đáp ứng được những nhu cầu tiên tiến và đột phá hơn.

IPv6 và 5G được xem là đang làm thay đổi hệ sinh thái mạng. Việc nhận thức về sự thay đổi này sẽ mang lại cơ hội và lợi thế khi hòa nhập xu thế đi trước thời cuộc như của một số nhà mạng. Vì thế việc phát triển 5G tại Việt Nam cần có lộ trình phát triển phù hợp và tối ưu nhất dựa trên kinh nghiệm triển khai của các nhà mạng trên thế giới.

KẾT LUẬN

IoT, 5G là một hệ sinh thái, được phát triển và có sự gắn kết với nhau. Sự phát triển gần đây cho thấy xu thế rõ ràng của sự hội tụ mạnh mẽ giữa IoT, 5G và IPv6. IPv6 sẽ cung cấp cho Internet of Things khả năng mở rộng, hỗ trợ khả năng tương tác, khả năng bảo mật; IPv6 được thiết kế phù hợp với dịch vụ di động cũng như hệ sinh thái của 5G và IoT.

Trên cơ sở các chính sách kịp thời và hiệu quả, Việt Nam về cơ bản đã chuyển đổi thành công mạng Internet sang hoạt động với thế hệ địa chỉ mới IPv6 và hiện đang đứng ở vị trí top đầu các nước có tỉ lệ ứng dụng IPv6 cao nhất toàn cầu (thứ 8 toàn cầu, thứ 2 khu vực ASEAN, thứ 3 châu Á. Tỷ lệ sử dụng IPv6 đạt 50% với hơn 50 triệu người sử dụng Internet qua IPv6, gấp 2,3 lần bình quân khu vực ASEAN; 1,7 lần bình quân toàn cầu). Mặc dù vậy, hiện chưa có các kết quả ứng dụng triển khai IPv6 trên các dịch vụ công nghệ mới (nội dung số, cloud, 5G, IoT) – đây là điểm khác biệt với tình hình quốc tế.

Trước thực trạng IPv4 hoàn toàn cạn kiệt, ứng dụng IPv6 là giải pháp duy nhất để phát triển mạng, dịch vụ, trong thời gian tới, vẫn cần thêm các hoạt động thúc đẩy triển khai IPv6 toàn diện trên hoạt động Internet Việt Nam, đồng thời xúc tiến ứng dụng IPv6 trên các dịch vụ nội dung, cloud, 5G, IoT để đảm bảo Việt Nam tiếp tục đi cùng với xu thế công nghệ toàn cầu.

Tài liệu này đã khái quát hóa về hiện trạng chuyển đổi Internet sang thế hệ mới hoạt động với IPv6; hiện trạng và xu thế triển khai IPv6 cho IoT; Việc xây dựng tiêu chuẩn hóa cho Ipv6 cho IoT; Các phương pháp phân hoạch và đánh số IPv6 dành cho IoT; Kỹ thuật định tuyến IPv6 cho IoT. Trên cơ sở đó, đưa ra các khuyến nghị liên quan tới các thành viên địa chỉ.

Các nội dung tài liệu phần nào hỗ trợ cho các tổ chức, doanh nghiệp Việt Nam trong công tác sử dụng địa chỉ IPv6 nói chung, ứng dụng IPv6 cho IoT nói riêng trong xu thế công nghệ, dịch vụ mới.

TÀI LIỆU THAM KHẢO

[1] Thông tin công bố tại Website của các tổ chức:

www.apnic.net

www.ripe.net

www.cisco.com

www.google.com

www.vnnic.vn.

www.ipv6.vn

[2] Thông tin công bố tại các địa chỉ, tài liệu sau:

1. A Survey of IPv6 Addressing Schemes for Internet of Things: https://www.researchgate.net/publication/

2. Deployment of IPv6-based Internet of Things: https://www.etsi.org/deliver/etsi_gr/IP6/001_099/008/01.01.01_60/gr_ip6008v010101p.pdf

3. IoT – IPv6 Intergration handbook for SMEs: https://iot6.eu/handbook

5. Dự án IoT6 của EU: http://www.iot6.eu.

6. ETSI IPv6 Enhanced Innovation report: https://www.etsi.org/deliver/etsi_gr/IPE/001_099/001/01.01.01_60/gr_IPE001v010101p.pdf

7. IPv6 Addressing Strategies for IoT: https://ieeexplore.ieee.org/document/6507541/citations#citations

8. A New Hybrid Method of IPv6 Addressing in the Internet of Things: https://arxiv.org/ftp/arxiv/papers/1811/1811.01178.pdf.

9. Reference model of IPv6 subnet addressing plan for Internet of things deployment.

10. https://vietnamnet.vn/vn/cong-nghe/vien-thong/cong-bo-chuong-trinh-ho-tro-chuyen-doi-sang-ipv6-cho-co-quan-nha-nuoc-den-nam-2025-705889.html

11. https://www.aelius.com/njh/google-ipv6/

12. https://www.arin.net/blog/2020/03/04/u-s-federal-government-plans-for-ipv6-only-readiness/

13. https://www.stackscale.com/blog/china-plan-ipv6-adoption/

14. https://gsacom.com/paper/5g-ecosystem-february-2022/

15. https://gsacom.com/paper/nts-statistics-february-2022/

16. https://asia.nikkei.com/Spotlight/5G-networks/China-s-5G-network-to-reach-2m-base-stations-this-year

17. https://gsacom.com/paper/5g-standalone-january-2022-member-report-with-annex/

18. https://www.t-mobile.com/content/dam/tfb/pdf/TFB_TechTarget-whitepaper_SA-NSA-5G.pdf?icid=TFB_TMO_P_20CONTENT_EFTB9174KOUY53MNG23700.

19. https://www.extremetech.com/mobile/127213-ipv6-now-deployed-across-entire-t-mobile-us-network

20. https://www.internetsociety.org/resources/deploy360/2014/case-study-t-mobile-us-goes-ipv6-only-using-464xlat/

21. https://www.tmonews.com/2019/06/t-mobile-galaxy-s10-5g-launch-network-six- cities/

22. https://www.t-mobile.com/news/network/standalone-5g-launch

23. https://www.samsung.com/global/business/networks/insights/white-papers/0107-5g-standalone-architecture/

24. https://www.etsi.org/newsroom/news/1814-2020-08-etsi-ipv6-white-paper-outlines-best-practices-challenges-benefits-and-the-way-forward

25. https://www.apnic.net/wp-content/uploads/2017/01/IPv6_Migration_Strategies_for_Mobile_Networks_Whitepaper.pdf

26. https://developer.apple.com/support/ipv6/

27. https://www.esnog.net/gore20/gore20-files/ipv6-cellular_v6.pdf

28. https://www.mobileworldlive.com/asia/asia-news/china-5g-connection-growth-continues

29. http://www.cac.gov.cn/2021-11/25/c_1639439849620158.htm

30. https://www.iab.org/2016/11/07/iab-statement-on-ipv6/

31. https://www.osti.gov/biblio/1642737

PHỤ LỤC 1: TRIỂN KHAI MÔ HÌNH PHÂN HOẠCH ĐỊA CHỈ THEO CÁC TIỀN TỐ ĐỊNH TUYẾN TOÀN CẦU

1. Tiền tố /56

Mô hình như sau:

Bảng 1: Bảng phân hoạch tiền tố /56

	Range			Dual IPv4 IPv6 Range			
						IPv4	
Allocation	A	B	Nb	A	B	octet	Nb
DMZ	0	0-f	32	0	0-f	0 - 15	32
	1	0-f		1	0-f	16 - 31	
Internal Servers	2	0-f	32	2	0-f	32 - 47	32
	3	0-f		3	0-f	48 - 63	
Default LAN	4	0-f	64	4	0-f	64 - 79	64
	5	0-f		5	0-f	80 - 95	
	6	0-f		6	0-f	96 - 111	
	7	0-f		7	0-f	112 - 127	
Internet of Things	8	0-f	64	8	0-f	128 - 143	64
	9	0-f		9	0-f	144 - 159	
	a	0-f		a	0-f	160 - 175	
	b	0-f		b	0-f	176 - 191	
Reserved & Others	c	0-f	64	c	0-f	192 - 207	64
	d	0-f		d	0-f	208 - 223	
	e	0-f		e	0-f	224 - 239	
	f	0-f		f	0-f	240 - 255	
			256				256

2. Tiền tố /44

Mô hình như sau:

Bảng 2: Bảng phân hoạch cho tiền tố /44

							Dual IPv6 - IPv4 Range							IPv6 Only Range					
	IPv6						IPv6					IPv4		IPv6					
Allocation	A	B	C	D	E	Nb	A	B	C	D	E	octet B-C	octet D-E	Nb	A	B	C	D	E	Nb
DMZ	0-f	0	0-f	0-f	0-f	2^17	0	0	0-f	0-f	0-f	0 - 15	0-255	2^13	0-f	0	0-f	0-f	0-f	2^21
	0-f	1	0-f	0-f	0-f		0	1	0-f	0-f	0-f	16 - 31	0-256		0-f	1	0-f	0-f	0-f	
Internal Servers	0-f	2	0-f	0-f	0-f	2^17	0	2	0-f	0-f	0-f	32 - 47	0-256	2^13	0-f	2	0-f	0-f	0-f	2^21
	0-f	3	0-f	0-f	0-f		0	3	0-f	0-f	0-f	48 - 63	0-256		0-f	3	0-f	0-f	0-f	
Default LAN	0-f	4	0-f	0-f	0-f	2^18	0	4	0-f	0-f	0-f	64 - 79	0-256	2^14	0-f	4	0-f	0-f	0-f	2^22
	0-f	5	0-f	0-f	0-f		0	5	0-f	0-f	0-f	80 - 95	0-256		0-f	5	0-f	0-f	0-f	
	0-f	6	0-f	0-f	0-f		0	6	0-f	0-f	0-f	96 - 111	0-256		0-f	6	0-f	0-f	0-f	
	0-f	7	0-f	0-f	0-f		0	7	0-f	0-f	0-f	112 - 127	0-256		0-f	7	0-f	0-f	0-f	
Internet of Things	0-f	8	0-f	0-f	0-f	2^18	0	8	0-f	0-f	0-f	128 - 143	0-256	2^14	0-f	8	0-f	0-f	0-f	2^22
	0-f	9	0-f	0-f	0-f		0	9	0-f	0-f	0-f	144 - 159	0-256		0-f	9	0-f	0-f	0-f	
	0-f	a	0-f	0-f	0-f		0	a	0-f	0-f	0-f	160 - 175	0-256		0-f	a	0-f	0-f	0-f	
	0-f	b	0-f	0-f	0-f		0	b	0-f	0-f	0-f	176 - 191	0-256		0-f	b	0-f	0-f	0-f	
Reserved & Others	0-f	c	0-f	0-f	0-f	2^18	0	c	0-f	0-f	0-f	192 - 207	0-256	2^14	0-f	c	0-f	0-f	0-f	2^22
	0-f	d	0-f	0-f	0-f		0	d	0-f	0-f	0-f	208 - 223	0-256		0-f	d	0-f	0-f	0-f	
	0-f	e	0-f	0-f	0-f		0	e	0-f	0-f	0-f	224 - 239	0-256		0-f	e	0-f	0-f	0-f	
	0-f	f	0-f	0-f	0-f		0	f	0-f	0-f	0-f	240 - 255	0-256		0-f	f	0-f	0-f	0-f	
						2^20								2^16						2^24

3. Tiền tố /40

Mô hình như sau:

Bảng 3: Bảng phân hoạch cho tiền tố /40

	Dual IPv6 - IPv4 Range									IPv6 Only Range							
	IPv6						IPv4			IPv6							
Allocation	A	B	C	D	E	F	octet C-D	octet E-F	Nb	A	B	C	D	E	F	Nb
DMZ	0	0	0	0-f	0-f	0-f	0 - 15	0-255	2^13	0-f	0-f	0	0-f	0-f	0-f	2^21
	0	0	1	0-f	0-f	0-f	16 - 31	0-256		0-f	0-f	1	0-f	0-f	0-f	
Internal Servers	0	0	2	0-f	0-f	0-f	32 - 47	0-256	2^13	0-f	0-f	2	0-f	0-f	0-f	2^21
	0	0	3	0-f	0-f	0-f	48 - 63	0-256		0-f	0-f	3	0-f	0-f	0-f	
Default LAN	0	0	4	0-f	0-f	0-f	64 - 79	0-256	2^14	0-f	0-f	4	0-f	0-f	0-f	2^22
	0	0	5	0-f	0-f	0-f	80 - 95	0-256		0-f	0-f	5	0-f	0-f	0-f	
	0	0	6	0-f	0-f	0-f	96 - 111	0-256		0-f	0-f	6	0-f	0-f	0-f	
	0	0	7	0-f	0-f	0-f	112 - 127	0-256		0-f	0-f	7	0-f	0-f	0-f	
Internet of Things	0	0	8	0-f	0-f	0-f	128 - 143	0-256	2^14	0-f	0-f	8	0-f	0-f	0-f	2^22
	0	0	9	0-f	0-f	0-f	144 - 159	0-256		0-f	0-f	9	0-f	0-f	0-f	
	0	0	a	0-f	0-f	0-f	160 - 175	0-256		0-f	0-f	a	0-f	0-f	0-f	
	0	0	b	0-f	0-f	0-f	176 - 191	0-256		0-f	0-f	b	0-f	0-f	0-f	
Reserved & Others	0	0	c	0-f	0-f	0-f	192 - 207	0-256	2^14	0-f	0-f	c	0-f	0-f	0-f	2^22
	0	0	d	0-f	0-f	0-f	208 - 223	0-256		0-f	0-f	d	0-f	0-f	0-f	
	0	0	e	0-f	0-f	0-f	224 - 239	0-256		0-f	0-f	e	0-f	0-f	0-f	
	0	0	f	0-f	0-f	0-f	240 - 255	0-256		0-f	0-f	f	0-f	0-f	0-f	
									2^16								2^24

4. Tiền tố /36

Mô hình như sau:

Bảng 4: Bảng phân hoạch cho tiền tố /40

	Address Range								Dual IPv6 - IPv4										Pure IPv6							
	IPv6								IPv6							IPv4			IPv6							
Allocation	A	B	C	D	E	F	G	Nb	A	B	C	D	E	F	G	octet C-D	octet E-F	Nb	A	B	C	D	E	F	G	Nb
DMZ	0-f	0-f	**0**	0-f	0-f	0-f	0-f	2^25	0	0	**0**	0-f	0-f	0-f	0	0 - 15	0-255	2^13	0-f	0-f	**0**	0-f	0-f	0-f	0-f	2^25
	0-f	0-f	**1**	0-f	0-f	0-f	0-f		0	0	**1**	0-f	0-f	0-f	0	16 - 31	0-256		0-f	0-f	**1**	0-f	0-f	0-f	0-f	
Internal Servers	0-f	0-f	**2**	0-f	0-f	0-f	0-f	2^25	0	0	**2**	0-f	0-f	0-f	0	32 - 47	0-256	2^13	0-f	0-f	**2**	0-f	0-f	0-f	0-f	2^25
	0-f	0-f	**3**	0-f	0-f	0-f	0-f		0	0	**3**	0-f	0-f	0-f	0	48 - 63	0-256		0-f	0-f	**3**	0-f	0-f	0-f	0-f	
Default LAN	0-f	0-f	**4**	0-f	0-f	0-f	0-f	2^26	0	0	**4**	0-f	0-f	0-f	0	64 - 79	0-256	2^14	0-f	0-f	**4**	0-f	0-f	0-f	0-f	2^26
	0-f	0-f	**5**	0-f	0-f	0-f	0-f		0	0	**5**	0-f	0-f	0-f	0	80 - 95	0-256		0-f	0-f	**5**	0-f	0-f	0-f	0-f	
	0-f	0-f	**6**	0-f	0-f	0-f	0-f		0	0	**6**	0-f	0-f	0-f	0	96 - 111	0-256		0-f	0-f	**6**	0-f	0-f	0-f	0-f	
	0-f	0-f	**7**	0-f	0-f	0-f	0-f		0	0	**7**	0-f	0-f	0-f	0	112 - 127	0-256		0-f	0-f	**7**	0-f	0-f	0-f	0-f	
Internet of Things	0-f	0-f	**8**	0-f	0-f	0-f	0-f	2^26	0	0	**8**	0-f	0-f	0-f	0	128 - 143	0-256	2^14	0-f	0-f	**8**	0-f	0-f	0-f	0-f	2^26
	0-f	0-f	**9**	0-f	0-f	0-f	0-f		0	0	**9**	0-f	0-f	0-f	0	144 - 159	0-256		0-f	0-f	**9**	0-f	0-f	0-f	0-f	
	0-f	0-f	**a**	0-f	0-f	0-f	0-f		0	0	**a**	0-f	0-f	0-f	0	160 - 175	0-256		0-f	0-f	**a**	0-f	0-f	0-f	0-f	
	0-f	0-f	**b**	0-f	0-f	0-f	0-f		0	0	**b**	0-f	0-f	0-f	0	176 - 191	0-256		0-f	0-f	**b**	0-f	0-f	0-f	0-f	
Reserved & Others	0-f	0-f	**c**	0-f	0-f	0-f	0-f	2^26	0	0	**c**	0-f	0-f	0-f	0	192 - 207	0-256	2^14	0-f	0-f	**c**	0-f	0-f	0-f	0-f	2^26
	0-f	0-f	**d**	0-f	0-f	0-f	0-f		0	0	**d**	0-f	0-f	0-f	0	208 - 223	0-256		0-f	0-f	**d**	0-f	0-f	0-f	0-f	
	0-f	0-f	**e**	0-f	0-f	0-f	0-f		0	0	**e**	0-f	0-f	0-f	0	224 - 239	0-256		0-f	0-f	**e**	0-f	0-f	0-f	0-f	
	0-f	0-f	**f**	0-f	0-f	0-f	0-f		0	0	**f**	0-f	0-f	0-f	0	240 - 255	0-256		0-f	0-f	**f**	0-f	0-f	0-f	0-f	
								2^28										2^16								2^28

PHỤ LỤC 2: DANH SÁCH RFC LIÊN QUAN IPV6, IOT, 5G

[1] IETF RFC 4861: "Neighbor Discovery for IP version 6".

[2] IETF RFC 4862: "IPv6 Stateless Address Autoconfiguration".

[3] IETF RFC 8499: "DNS Terminology".

[4] IETF RFC 8415: "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)".

[5] IETF RFC 8028: "First-Hop Router Selection by Hosts in a Multi-Prefix Network".

[6] IETF RFC 8200: "Internet Protocol, Version 6 (IPv6) Specification".

[7] IETF RFC 8981: "Temporary Address Extensions for Stateless Address Autoconfiguration in IPv6".

[8] IETF RFC 6724: "Default Address Selection for Internet Protocol Version 6 (IPv6)".

[9] IETF RFC 7610: "DHCPv6-Shield: Protecting against Rogue DHCPv6 Servers".

[10] IETF RFC 6105: "IPv6 Router Advertisement Guard".

[11] IETF RFC 6877: "Combination of Stateful and Stateless Translation".

[12] IETF RFC 7597: "Mapping of Address and Port with Encapsulation (MAP-E)".

[13] IETF RFC 7599: "Mapping of Address and Port using Translation".

[14] IETF RFC 6333: "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion".

[15] IETF RFC 7596: "Lightweight 4over6: An Extension to the Dual-Stack Lite Architecture".

[16] IETF RFC 7252: "The Constrained Application Protocol (CoAP)".

[17] IETF RFC 7799: "Active and Passive Metrics and Methods (with Hybrid Types In-Between)".

[18] IETF draft-jdurand-ipv6-multicast-ra: "Route Advertisement Option for IPv6 Multicast Prefixes".

[19] IETF draft-pfister-moving-net-autoconf: "Routers auto-configuration using Route Information Option from ICMPv6 Router Advertisements".

[20] IDC FutureScape Highlights. Các tài liệu có tại địa chỉ:

https://www.idc.com/getdoc.jsp?containerId=prUS46963620.

[21] IETF draft-ietf-v6ops-IPv6-deployment-status: "IPv6 Deployment Status".

[22] IETF RFC 7368: "IPv6 Home Networking Architecture Principles".

[23] IETF RFC 7157: "IPv6 Multihoming without Network Address Translation".

[24] IETF draft-ietf-6man-grand: "Gratuitous Neighbor Discovery: Creating Neighbor Cache Entries on First-Hop Routers".

[25] draft-pref64folks-6man-ra-pref64: "Discovering PREF64 in Router Advertisements".

[26] IETF RFC 8106: "IPv6 Router Advertisement Options for DNS Configuration".

[27] IETF RFC 5175: "IPv6 Router Advertisement Flags Option".

[28] GoogleTM IPv6 statistics NOTE: Available at https://www.google.com/intl/en/ipv6/statistics.html.

[29] draft-ietf-idr-bgpls-srv6-ext: "BGP Link State Extensions for SRv6".

[30] IETF draft-ioametal-ippm-6man-ioam-ipv6-deployment: "Deployment Considerations for In-situ OAM with IPv6 Options".

[31] IETF RFC 8979: "Reaction of IPv6 Stateless Address Autoconfiguration (SLAAC) to FlashRenumbering Events".

[32] IETF RFC 8660: "Segment Routing with the MPLS Data Plane".

[33] IETF RFC 8754: "IPv6 Segment Routing Header (SRH)".

[34] IETF RFC 8986: "Segment Routing over IPv6 (SRv6) Network Programming".

[35] IETF RFC 6146: "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers".

[36] IETF RFC 6052: "IPv6 Addressing of IPv4/IPv6 Translators".

[37] IETF RFC 7915: "IP/ICMP Translation Algorithm".

[38] IETF RFC 8402: "Segment Routing Architecture".

[39] IETF RFC 3031: "Multiprotocol Label Switching Architecture".

[40] IETF RFC 7348: "Virtual eXtensible Local Area Network (VXLAN): A Framework for Overlaying Virtualized Layer 2 Networks over Layer 3 Networks".

[41] IETF draft-ietf-lsr-isis-sr-vtn-mt: "Using IS-IS Multi-Topology (MT) for Segment Routing based Virtual Transport Network".

[42] IETF RFC 7011: "Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of Flow Information". Tài liệu có tại địa chỉ: https://datatracker.ietf.org/doc/html/rfc7011.

[43] IETF RFC 8321: "Alternate-Marking Method for Passive and Hybrid Performance Monitoring".

[44] IETF draft-ietf-ippm-ioam-ipv6-options: "In-situ OAM IPv6 Options".

CHÚ THÍCH: Tài liệu có tại địa chỉ: https://tools.ietf.org/html/draft-ietf-ippm-ioam-ipv6-options-04.

[45] IETF RFC 7039: "Source Address Validation Improvement (SAVI) Framework".

[46] OIF FLEXE-02.1: "Flexible Ethernet 2.1 Implementation Agreement".

[47] IETF draft-kumar-rtgwg-grpc-protocol: "gRPC Protocol".

[48] IETF draft-openconfig-rtgwg-gnmi-spec: "gRPC Network Management Interface (gNMI)".

[49] IETF draft-ietf-opsawg-ntf: "Network Telemetry Framework".

[50] IETF draft-ietf-bier-use-cases: "BIER Use Cases".

[51] IETF draft-ietf-idr-segment-routing-te-policy: "Advertising Segment Routing Policies in BGP".

[52] IETF RFC 7217: "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)".

[53] IETF draft-ietf-opsec-v6-27: "Operational Security Considerations for IPv6 Networks".

[54] IETF RFC 2236: "Internet Group Management Protocol, Version 2".

[55] IETF RFC 3376: "Internet Group Management Protocol, Version 3".

[56] IETF RFC 2475: "An Architecture for Differentiated Services".

[57] IETF RFC 1633: "Integrated Services in the Internet Architecture: an Overview".

[58] IEEE 802.15.4™: "Low-rate wireless personal area networks".

[59] IETF draft-ietf-pce-segment-routing-ipv6: "PCEP Extensions for Segment Routing leveraging the IPv6 data plane".

[60] IETF RFC 8955: "Dissemination of Flow Specification Rules".

[61] IETF RFC 7209: "Requirements for Ethernet VPN (EVPN)".

[62] IETF RFC 7432: "BGP MPLS-Based Ethernet VPN".

[63] IETF RFC 8214: "Virtual Private Wire Service Support in Ethernet VPN".

[64] IETF draft-ietf-teas-enhanced-vpn: "A Framework for Enhanced Virtual Private Network (VPN+) Services".

[65] IETF draft-ietf-spring-resource-aware-segments: "Introducing Resource Awareness to SR Segments".

[66] IETF RFC 8724: "SCHC: Generic Framework for Static Context Header Compression and Fragmentation".

[67] ETSI White Paper #35: "IPv6 Best Practices, Benefits, Transition Challenges and the Way Forward".

[68] Compendium on IPv6 Based Solutions/Architecture/Case Studies for Different Industry Verticals "National IPv6 Deployment Roadmap version II" in India. Tài liệu có tại địa chỉ:

https://dot.gov.in/sites/default/files/Compendium_on_IPv6_Based_Solutions.pdf.
ETSI 12 ETSI GR IPE 001 V1.1.1 (2021-08)

[69] ETSI GR IP6 001 (V1.1.1): "IPv6 Deployment in the enterprise".

[70] IETF RFC 7381: "Enterprise IPv6 Deployment Guidelines".

[71] IETF RFC 8466: "A YANG Data Model for Layer 2 Virtual Private Network (L2VPN) Service Delivery".

[72] IETF RFC 8299: "YANG Data Model for L3VPN Service Delivery".

[73] IETF draft-ietf-lsr-flex-algo: "IGP Flexible Algorithm".

[74] IETF RFC 2710: "Multicast Listener Discovery (MLD) for IPv6".

[75] IETF RFC 7761: "Protocol Independent Multicast - Sparse Mode (PIM-SM)".

[76] IETF RFC 6513: "Multicast in MPLS/BGP IP VPNs".

[77] IETF RFC 1918: "Address Allocation for Private Internets".

[78] IETF RFC 6037: "Cisco Systems' Solution for Multicast in BGP/MPLS IP VPNs".

[79] IETF RFC 7113: "RFC 7113 - Implementation Advice for IPv6 Router Advertisement Guard".

[80] IETF RFC 7872: "Observations on the Dropping of Packets with IPv6 Extension Headers in the Real World".

[81] IETF RFC 5578: "PPP over Ethernet (PPPoE) Extensions for Credit Flow and Link Metrics".

[82] ETSI TS 129 281: "Universal Mobile Telecommunications System (UMTS); LTE; 5G; General Packet Radio System (GPRS) Tunnelling Protocol User Plane (GTPv1-U) (3GPP TS 29.281)".

[83] BBF TR-177: "IPv6 in the context of TR-101".

[84] IETF RFC 7084: "Basic Requirements for IPv6 Customer Edge Router".

[85] IETF RFC 8585: "Requirements for IPv6 Customer Edge Routers to Support IPv4-as-a-Service".

[86] IETF RFC 8305: "Happy Eyeballs Version 2: Better Connectivity Using Concurrency".

[87] BBF TR-187: "IPv6 for PPP Broadband Access".

[88] IEEE 802.1Q™: "IEEE Standard for Local and Metropolitan Area Networks-Bridges and Bridged Networks".

[89] IETF RFC 6775: "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)".

[90] IETF RFC 8505: "Registration Extensions for IPv6 over Low-Power Wireless Personal Area Network (6LoWPAN) Neighbor Discovery".

[91] IETF RFC 8928: "Address-Protected Neighbor Discovery for Low-Power and Lossy Networks".

[92] IETF RFC 8929: "IPv6 Backbone Router".

[93] IETF RFC 4291: "IP Version 6 Addressing Architecture".

[94] IETF RFC 6830: "The Locator/ID Separation Protocol".

[95] IETF draft-ietf-rift-rift: "RIFT: Routing in Fat Trees".

[96] ETF IETF RFC 7668: "IPv6 over BLUETOOTH® Low Energy".

[97] IETF RFC 6550: "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks".

[98] IETF RFC 9010: "Routing for RPL (Routing Protocol for Low-Power and Lossy Networks) Leaves".

[99] IETF RFC 6762: "Multicast DNS". ETSI 13 ETSI GR IPE 001 V1.1.1 (2021-08)

[100] IETF RFC 5942: "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes".

[101] IETF draft-ietf-6man-spring-srv6-oam: "Operations, Administration, and Maintenance (OAM) in Segment Routing Networks with IPv6 Data plane (SRv6)".

[102] IETF draft-yourtchenko-6man-dad-issues: "A survey of issues related to IPv6 Duplicate Address Detection".

[103] IETF RFC 3971: "SEcure Neighbor Discovery (SEND)".

[104] IETF RFC 3972: "Cryptographically Generated Addresses (CGA)".

[105] IETF BCP 38: "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing".

[106] IETF RFC 6959: "Source Address Validation Improvement (SAVI) Threat Scope".

[107] IETF RFC 8074: "Source Address Validation Improvement (SAVI) for Mixed Address Assignment Methods Scenario".

[108] IEEE 802.11™: "IEEE Standard for Information technology -- Telecommunications and information exchange between systems Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification".

[109] IEEE 802.11s™: "IEEE Standard for Information Technology -- Telecommunications and information exchange between systems -- Local and metropolitan area networks -- Specific requirements -- Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications Amendment 10: Mesh Networking".

[110] IEEE 802.15.10™: "IEEE Recommended Practice for Routing Packets in IEEE 802.15.4 Dynamically Changing Wireless Networks".

[111] W3Tech. Tài liệu có tại địa chỉ: https://w3techs.com/technologies/overview/site_element.

[112] IPv6 Deployment Aggregated Status. Tài liệu có tại địa chỉ: https://www.vyncke.org/ipv6status/index.php?small-samples=on.

[113] APNIC.

CHÚ THÍCH: Tài liệu có tại địa chỉ: https://stats.labs.apnic.net/ipv6.

[114] ARCEP: "Annual Barometer of the transition to IPv6 in France" . Tài liệu có tại địa chỉ: https://www.arcep.fr/fileadmin/reprise/observatoire/ipv6/Arcep_2020_Barometer_of_the_Transition_to_I Pv6_dec2020.pdf.

[115] Akamai: "IPv6 Adoption By Country". Tài liệu có tại địa chỉ: https://www.akamai.com/us/en/resources/our-thinking/state-of-the-internet-report/state-ofthe-internet-ipv6-adoption-visualization.jsp.

[116] ETSI GS MEC 001: "Multi-access Edge Computing (MEC); Terminology".

[117] ETSI GS MEC 002: "Multi-access Edge Computing (MEC); Phase 2: Use Cases and Requirements".

[118] ETSI GS MEC 003: "Multi-access Edge Computing (MEC); Framework and Reference Architecture".

[119] IETF draft-ietf-bier-mld: "BIER Ingress Multicast Flow Overlay using Multicast Listener Discovery Protocols". ETSI 14 ETSI GR IPE 001 V1.1.1 (2021-08)

[120] IETF RFC 6514: "BGP Encodings and Procedures for Multicast in MPLS/BGP IP VPNs".

[121] IETF RFC 8279: "Multicast Using Bit Index Explicit Replication (BIER)".

[122] IETF RFC 8296: "Encapsulation for Bit Index Explicit Replication (BIER) in MPLS and Non-MPLS Networks".

[123] IETF draft-ietf-bier-ipv6-requirements: "BIER IPv6 Requirements".

[124] IETF draft-ietf-bier-problem-statement: "Bit Indexed Explicit Replication (BIER) Problem Statement".

[125] IETF RFC 8556: "Multicast VPN Using Bit Index Explicit Replication (BIER)".

[126] draft-ietf-bier-bierin6: "Supporting BIER in IPv6 Networks (BIERin6)".

[127] IETF RFC 8534: "Explicit Tracking with Wildcard Routes in Multicast VPN".

[128] IETF RFC 8401: "Bit Index Explicit Replication (BIER) Support via IS-IS".

[129] IETF RFC 8444: "OSPFv2 Extensions for Bit Index Explicit Replication (BIER)".

[130] IETF draft-ietf-bess-srv6-services: "SRv6 BGP based Overlay Services".

[131] IETF draft-ietf-bier-oam-requirements: "Operations, Administration and Maintenance (OAM) Requirements for Bit Index Explicit Replication (BIER) Layer".

[132] IETF draft-ietf-bier-pmmm-oam: "Performance Measurement (PM) with Marking Method in Bit Index Explicit Replication (BIER) Layer".

[133] IETF RFC 4176: "Framework for Layer 3 Virtual Private Networks (L3VPN) Operations and Management".

[134] IETF RFC 4364: "BGP/MPLS IP Virtual Private Networks (VPNs)".

[135] IETF RFC 4664: "Framework for Layer 2 Virtual Private Networks (L2VPNs)".

[136] IETF RFC 6624: "Layer 2 Virtual Private Networks Using BGP for Auto-Discovery and Signaling".

[137] IETF RFC 8077: "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)".

[138] IETF RFC 4448: "Encapsulation Methods for Transport of Ethernet over MPLS Networks".

[139] IETF RFC 4761: "Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling".

[140] IETF RFC 4762: "Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling".

[141] IETF draft-ietf-spring-sr-for-enhanced-vpn: "Segment Routing based Virtual Transport Network (VTN) for Enhanced VPN".

[142] China IPv6 statistics. Tài liệu có tại địa chỉ: https://www.china-ipv6.cn/#/.

[143] IETF draft-ietf-idr-sr-policy-ifit: "BGP SR Policy Extensions to Enable IFIT".

[144] IETF draft-ietf-netconf-distributed-notif: "Subscription to Distributed Notifications".

[145] IETF draft-ietf-ippm-ioam-yang: "A YANG Data Model for In-Situ OAM".

[146] ETSI GR IP6 031 (V1.1.1): "IPv6 Security, Cybersecurity, Blockchain". [147] ETSI GR IP6 006 (V1.1.1): "Generic migration steps from IPv4 to IPv6". ETSI 15 ETSI GR IPE 001 V1.1.1 (2021-08)

[148] ETSI GR IP6 010 (V1.1.1): "IPv6-based SDN and NFV; Deployment of IPv6-based SDN and NFV".

[149] IETF draft-ietf-sunset4-ipv6-ietf-01: "IETF: End Work on IPv4".