TCVN T I Ê U C H U Ẩ N Q U Ố C G I A

**TCVN xxxx:202x**

**CÁC YÊU CẦU ĐỐI VỚI THIẾT BỊ NÚT IPv6**

***IPv6 Node Requirements***

**HÀ NỘI - 2022**

|  |
| --- |
| **Lời nói đầu**  TCVN xxxx:202x được xây dựng trên cơ sở tham khảo tài liệu RFC 8504 (2019) “IPv6 Node Requirements” của Nhóm đặc trách kỹ thuật Internet (IETF) và rà soát chuyển đổi Quy chuẩn kỹ thuật quốc gia QCVN 89:2015/BTTTT.  TCVN xxxx:202x do Viện Khoa học Kỹ thuật Bưu điện - Học viện Công nghệ Bưu chính Viễn thông biên soạn, Bộ Thông tin và Truyền thông đề nghị, Tổng cục Tiêu chuẩn Đo lường chất lượng thẩm định, Bộ Khoa học và Công nghệ công bố. |

**MỤC LỤC**

[MỤC LỤC 1](#_Toc118987953)

[1 Phạm vi áp dụng 3](#_Toc118987954)

[2 Tài liệu viện dẫn 3](#_Toc118987955)

[3 Giải thích từ ngữ 6](#_Toc118987956)

[4 Các từ viết tắt sử dụng trong tiêu chuẩn 8](#_Toc118987957)

[5 Giới thiệu 8](#_Toc118987958)

[6 Tầng IP con 9](#_Toc118987959)

[7 Tầng IP 9](#_Toc118987960)

[7.1 Giao thức Internet phiên bản 6 – RFC 8200 9](#_Toc118987961)

[7.2 Hỗ trợ cho các tiêu đề mở rộng IPv6 10](#_Toc118987962)

[7.3 Bảo vệ nút khỏi các tùy chọn tiêu đề mở rộng quá mức 11](#_Toc118987963)

[7.4 Phát hiện nút mạng lân cận cho IPv6 - RFC 4861 11](#_Toc118987964)

[7.5 Phát hiện lân cận bảo mật (SEND) - RFC 3971 12](#_Toc118987965)

[7.6 Tùy chọn cờ quảng cáo bộ định tuyến IPv6 - RFC 5175 12](#_Toc118987966)

[7.7 Phát hiện đường dẫn MTU và kích cỡ gói 13](#_Toc118987967)

[7.8 ICMP cho giao thức Internet phiên bản 6 (IPv6) - RFC 4443 13](#_Toc118987968)

[7.9 Ưu tiên bộ định tuyến mặc định và các bộ định tuyến đặc trưng hơn - RFC 4191 13](#_Toc118987969)

[7.10 Lựa chọn bộ định tuyến chặng đầu tiên - RFC 8028 13](#_Toc118987970)

[7.11 Phát hiện lắng nghe truyền phát đa hướng (MLD) cho IPv6 – RFC 3810 14](#_Toc118987971)

[7.12 Thông báo tắc nghẽn rõ ràng (ECN) - RFC 3168 14](#_Toc118987972)

[8 Định địa chỉ và cấu hình địa chỉ 14](#_Toc118987973)

[8.1 Kiến trúc định địa chỉ IP phiên bản 6 – RFC 4291 14](#_Toc118987974)

[8.2 Khuyến nghị tính khả dụng của địa chỉ máy chủ 14](#_Toc118987975)

[8.3 Tự động cấu hình địa chỉ phi trạng thái IPv6 – RFC 4862 15](#_Toc118987976)

[8.4 Mở rộng quyền riêng tư cho cấu hình địa chỉ trong IPv6 - RFC 4941 15](#_Toc118987977)

[8.5 Tự động định cấu hình địa chỉ trạng thái (DHCPv6) - RFC 3315 16](#_Toc118987978)

[8.6 Lựa chọn địa chỉ mặc định cho IPv6 - RFC 6724 16](#_Toc118987979)

[9 Hệ thống tên miền (DNS) 16](#_Toc118987980)

[10 Định cấu hình thông tin không địa chỉ 16](#_Toc118987981)

[10.1 DHCP cho thông tin cấu hình khác 16](#_Toc118987982)

[10.2 Quảng cáo bộ định tuyến và cổng mặc định 17](#_Toc118987983)

[10.3 Tùy chọn quảng cáo bộ định tuyến IPv6 cho cấu hình DNS - RFC 8106 17](#_Toc118987984)

[10.4 Các tùy chọn DHCP so với tùy chọn quảng cáo bộ định tuyến cho cấu hình máy chủ 17](#_Toc118987985)

[11 Các giao thức phát hiện dịch vụ 17](#_Toc118987986)

[12 Hỗ trợ và chuyển đổi IPv4 18](#_Toc118987987)

[13 Hỗ trợ ứng dụng 18](#_Toc118987988)

[13.1 Thể hiện dạng văn bản địa chỉ IPv6 - RFC 5952 18](#_Toc118987989)

[13.2 Các giao diện lập trình ứng dụng (API) 18](#_Toc118987990)

[14 Tính di động 18](#_Toc118987991)

[15 Bảo mật 19](#_Toc118987992)

[15.1 Các yêu cầu 20](#_Toc118987993)

[15.2 Chuyển đổi và thuật toán 20](#_Toc118987994)

[16 Chức năng định tuyến cụ thể 20](#_Toc118987995)

[16.1 Tùy chọn cảnh báo định tuyến IPv6 - RFC 2711 20](#_Toc118987996)

[16.2 Phát hiện lân cận cho IPv6 - RFC 4861 20](#_Toc118987997)

[16.3 Tự động định cấu hình địa chỉ trạng thái (DHCPv6) - RFC 3315 20](#_Toc118987998)

[16.4 Khuyến nghị độ dài tiền tố IPv6 cho chuyển tiếp hướng thuận - BCP 198 21](#_Toc118987999)

[17 Thiết bị bị ràng buộc 21](#_Toc118988000)

[18 Quản lý nút IPv6 21](#_Toc118988001)

[18.1 Các mô đun cơ sở thông tin quản lý (MIB) 21](#_Toc118988002)

[18.2 Các mô hình dữ liệu YANG 22](#_Toc118988003)

[19 Các cân nhắc bảo mật 22](#_Toc118988004)

[20 Các cân nhắc IANA 22](#_Toc118988005)

[PHỤ LỤC A - CÁC THAY ĐỔI TỪ RFC 6434 23](#_Toc118988006)

[PHỤ LỤC B - CÁC THAY ĐỔI TỪ RFC 4294 tới RFC 6434 25](#_Toc118988007)

[THƯ MỤC TÀI LIỆU THAM KHẢO 26](#_Toc118988008)

**Các yêu cầu đối với thiết bị nút IPv6**

*IPv6 Node Requirements*

|  |  |
| --- | --- |
| **T I Ê U C H U Ẩ N Q U Ố C G I A** | **TCVN xxxx:202x** |

# Phạm vi áp dụng

Tiêu chuẩn này quy định các yêu cầu kỹ thuật đối với thiết bị nút IPv6.

Lưu ý rằng IPv6 gồm nhiều thông số kỹ thuật và sẽ được triển khai trong nhiều tình huống và môi trường khác nhau. Vì vậy, điều quan trọng là phải phát triển yêu cầu đối với các nút IPv6 để đảm bảo khả năng tương tác.

# Tài liệu viện dẫn

Tài liệu viện dẫn sau cần thiết cho việc áp dụng tiêu chuẩn này. Đối với các tài liệu viện dẫn ghi năm công bố thì áp dụng phiên bản được nêu. Đối với các tài liệu viện dẫn không ghi năm công bố thì áp dụng phiên bản mới nhất, bao gồm cả sửa đổi, bổ sung (nếu có).

[RFC1034] Mockapetris, P., "Domain names - concepts and facilities", STD 13, RFC 1034, DOI 10.17487/RFC1034, November 1987.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997.

[RFC2710] Deering, S., Fenner, W., and B. Haberman, "Multicast Listener Discovery (MLD) for IPv6", RFC 2710, DOI 10.17487/RFC2710, October 1999.

[RFC2711] Partridge, C. and A. Jackson, "IPv6 Router Alert Option", RFC 2711, DOI 10.17487/RFC2711, October 1999.

[RFC2863] McCloghrie, K. and F. Kastenholz, "The Interfaces Group MIB", RFC 2863, DOI 10.17487/RFC2863, June 2000.

[RFC3168] Ramakrishnan, K., Floyd, S., and D. Black, "The Addition of Explicit Congestion Notification (ECN) to IP", RFC 3168, DOI 10.17487/RFC3168, September 2001.

[RFC3315] Droms, R., Ed., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, DOI 10.17487/RFC3315, July 2003.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, DOI 10.17487/RFC3411, December 2002.

[RFC3596] Thomson, S., Huitema, C., Ksinant, V., and M. Souissi, "DNS Extensions to Support IP Version 6", STD 88, RFC 3596, DOI 10.17487/RFC3596, October 2003.

[RFC3736] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, DOI 10.17487/RFC3736, April 2004.

[RFC3810] Vida, R., Ed. and L. Costa, Ed., "Multicast Listener Discovery Version 2 (MLDv2) for IPv6", RFC 3810, DOI 10.17487/RFC3810, June 2004.

[RFC4033] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "DNS Security Introduction and Requirements", RFC 4033, DOI 10.17487/RFC4033, March 2005.

[RFC4034] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Resource Records for the DNS Security Extensions", RFC 4034, DOI 10.17487/RFC4034, March 2005.

[RFC4035] Arends, R., Austein, R., Larson, M., Massey, D., and S. Rose, "Protocol Modifications for the DNS Security Extensions", RFC 4035, DOI 10.17487/RFC4035, March 2005.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, DOI 10.17487/RFC4213, October 2005.

[RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing Architecture", RFC 4291, DOI 10.17487/RFC4291, February 2006.

[RFC4292] Haberman, B., "IP Forwarding Table MIB", RFC 4292, DOI 10.17487/RFC4292, April 2006.

[RFC4293] Routhier, S., Ed., "Management Information Base for the Internet Protocol (IP)", RFC 4293, DOI 10.17487/RFC4293, April 2006.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, DOI 10.17487/RFC4301, December 2005.

[RFC4303] Kent, S., "IP Encapsulating Security Payload (ESP)", RFC 4303, DOI 10.17487/RFC4303, December 2005.

[RFC4311] Hinden, R. and D. Thaler, "IPv6 Host-to-Router Load Sharing", RFC 4311, DOI 10.17487/RFC4311, November 2005.

[RFC4443] Conta, A., Deering, S., and M. Gupta, Ed., "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", STD 89, RFC 4443, DOI 10.17487/RFC4443, March 2006).

[RFC4607] Holbrook, H. and B. Cain, "Source-Specific Multicast for IP", RFC 4607, DOI 10.17487/RFC4607, August 2006.

[RFC4632] Fuller, V. and T. Li, "Classless Inter-domain Routing (CIDR): The Internet Address Assignment and Aggregation Plan", BCP 122, RFC 4632, DOI 10.17487/RFC4632, August 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, DOI 10.17487/RFC4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, DOI 10.17487/RFC4862, September 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, DOI 10.17487/RFC4941, September 2007.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, DOI 10.17487/RFC5095, December 2007.

[RFC5453] Krishnan, S., "Reserved IPv6 Interface Identifiers", RFC 5453, DOI 10.17487/RFC5453, February 2009.

[RFC5722] Krishnan, S., "Handling of Overlapping IPv6 Fragments", RFC 5722, DOI 10.17487/RFC5722, December 2009.

[RFC5790] Liu, H., Cao, W., and H. Asaeda, "Lightweight Internet Group Management Protocol Version 3 (IGMPv3) and Multicast Listener Discovery Version 2 (MLDv2) Protocols", RFC 5790, DOI 10.17487/RFC5790, February 2010.

[RFC5942] Singh, H., Beebee, W., and E. Nordmark, "IPv6 Subnet Model: The Relationship between Links and Subnet Prefixes", RFC 5942, DOI 10.17487/RFC5942, July 2010.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, DOI 10.17487/RFC5952, August 2010.

[RFC6241] Enns, R., Ed., Bjorklund, M., Ed., Schoenwaelder, J., Ed., and A. Bierman, Ed., "Network Configuration Protocol (NETCONF)", RFC 6241, DOI 10.17487/RFC6241, June 2011.

[RFC6437] Amante, S., Carpenter, B., Jiang, S., and J. Rajahalme, "IPv6 Flow Label Specification", RFC 6437, DOI 10.17487/RFC6437, November 2011).

[RFC6564] Krishnan, S., Woodyatt, J., Kline, E., Hoagland, J., and M. Bhatia, "A Uniform Format for IPv6 Extension Headers", RFC 6564, DOI 10.17487/RFC6564, April 2012.

[RFC6724] Thaler, D., Ed., Draves, R., Matsumoto, A., and T. Chown, "Default Address Selection for Internet Protocol Version 6 (IPv6)", RFC 6724, DOI 10.17487/RFC6724, September 2012.

[RFC6762] Cheshire, S. and M. Krochmal, "Multicast DNS", RFC 6762, DOI 10.17487/RFC6762, February 2013.

[RFC6763] Cheshire, S. and M. Krochmal, "DNS-Based Service Discovery", RFC 6763, DOI 10.17487/RFC6763, February 2013.

[RFC6775] Shelby, Z., Ed., Chakrabarti, S., Nordmark, E., and C. Bormann, "Neighbor Discovery Optimization for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)", RFC 6775, DOI 10.17487/RFC6775, November 2012.

[RFC6891] Damas, J., Graff, M., and P. Vixie, "Extension Mechanisms for DNS (EDNS(0))", STD 75, RFC 6891, DOI 10.17487/RFC6891, April 2013.

[RFC6946] Gont, F., "Processing of IPv6 "Atomic" Fragments", RFC 6946, DOI 10.17487/RFC6946, May 2013.

[RFC7045] Carpenter, B. and S. Jiang, "Transmission and Processing of IPv6 Extension Headers", RFC 7045, DOI 10.17487/RFC7045, December 2013.

[RFC7048] Nordmark, E. and I. Gashinsky, "Neighbor Unreachability Detection Is Too Impatient", RFC 7048, DOI 10.17487/RFC7048, January 2014.

[RFC7112] Gont, F., Manral, V., and R. Bonica, "Implications of Oversized IPv6 Header Chains", RFC 7112, DOI 10.17487/RFC7112, January 2014.

[RFC7217] Gont, F., "A Method for Generating Semantically Opaque Interface Identifiers with IPv6 Stateless Address Autoconfiguration (SLAAC)", RFC 7217, DOI 10.17487/RFC7217, April 2014.

[RFC7296] Kaufman, C., Hoffman, P., Nir, Y., Eronen, P., and T. Kivinen, "Internet Key Exchange Protocol Version 2 (IKEv2)", STD 79, RFC 7296, DOI 10.17487/RFC7296, October 2014.

[RFC7527] Asati, R., Singh, H., Beebee, W., Pignataro, C., Dart, E., and W. George, "Enhanced Duplicate Address Detection", RFC 7527, DOI 10.17487/RFC7527, April 2015.

[RFC7559] Krishnan, S., Anipko, D., and D. Thaler, "Packet-Loss Resiliency for Router Solicitations", RFC 7559, DOI 10.17487/RFC7559, May 2015.

[RFC7608] Boucadair, M., Petrescu, A., and F. Baker, "IPv6 Prefix Length Recommendation for Forwarding", BCP 198, RFC 7608, DOI 10.17487/RFC7608, July 2015.

[RFC8021] Gont, F., Liu, W., and T. Anderson, "Generation of IPv6 Atomic Fragments Considered Harmful", RFC 8021, DOI 10.17487/RFC8021, January 2017.

[RFC8028] Baker, F. and B. Carpenter, "First-Hop Router Selection by Hosts in a Multi-Prefix Network", RFC 8028, DOI 10.17487/RFC8028, November 2016.

[RFC8040] Bierman, A., Bjorklund, M., and K. Watsen, "RESTCONF Protocol", RFC 8040, DOI 10.17487/RFC8040, January 2017.

[RFC8064] Gont, F., Cooper, A., Thaler, D., and W. Liu, "Recommendation on Stable IPv6 Interface Identifiers", RFC 8064, DOI 10.17487/RFC8064, February 2017.

[RFC8106] Jeong, J., Park, S., Beloeil, L., and S. Madanapalli, "IPv6 Router Advertisement Options for DNS Configuration", RFC 8106, DOI 10.17487/RFC8106, March 2017.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017.

[RFC8200] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", STD 86, RFC 8200, DOI 10.17487/RFC8200, July 2017.

[RFC8201] McCann, J., Deering, S., Mogul, J., and R. Hinden, Ed., "Path MTU Discovery for IP version 6", STD 87, RFC 8201, DOI 10.17487/RFC8201, July 2017.

[RFC8221] Wouters, P., Migault, D., Mattsson, J., Nir, Y., and T. Kivinen, "Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH)", RFC 8221, DOI 10.17487/RFC8221, October 2017.

[RFC8247] Nir, Y., Kivinen, T., Wouters, P., and D. Migault, "Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 8247, DOI 10.17487/RFC8247, September 2017.

[RFC8343] Bjorklund, M., "A YANG Data Model for Interface Management", RFC 8343, DOI 10.17487/RFC8343, March 2018.

[RFC8344] Bjorklund, M., "A YANG Data Model for IP Management", RFC 8344, DOI 10.17487/RFC8344, March 2018.

# Giải thích từ ngữ

**3.1 Thiết bị nút IPv6**

Thiết bị thực thi IPv6. Thiết bị nút IPv6 bao gồm router IPv6 và host IPv6.

CHÚ THÍCH: Thuật ngữ thiết bị nút IPv6 (nút IPv6) tương đương với thuật ngữ nút mạng (Node) nêu tại mục 3.1 trong TCVN 9802-1:2013.

**3.2 Bộ định tuyến IPv6** (Router IPv6)

Thiết bị nút IPv6 có khả năng chuyển tiếp các gói tin IPv6 không được định địa chỉ rõ ràng cho thiết bị nút đó.

CHÚ THÍCH: Thuật ngữ router IPv6 (router) tương đương với thuật ngữ bộ định tuyến (Router) nêu tại mục 3.2 trong TCVN 9802-1:2013.

**3.3 Máy chủ IPv6** (Host IPv6)

Bất kỳ thiết bị nút IPv6 nào không phải là router IPv6.

CHÚ THÍCH: Thuật ngữ host IPv6 (host) tương đương với thuật ngữ máy chủ (host) nêu tại mục 3.3 trong TCVN 9802-1:2013.

**3.4 Địa chỉ liên kết cục bộ** (link-local address)

Địa chỉ unicast có phạm vi chỉ trong liên kết, được sử dụng để thông tin với các nút mạng lân cận.

**3.5 Phát hiện nút mạng lân cận**

Giao thức sử dụng để giải quyết các vấn đề liên quan đến sự tương tác giữa các nút mạng trên cùng một liên kết như phát hiện router, phát hiện tiền tố, phân giải địa chỉ.

CHÚ THÍCH: Thuật ngữ nút mạng lân cận sử dụng trong Quy chuẩn này tương đương với thuật ngữ nút láng giềng sử dụng trong TCVN 9802-1:2013.

**3.6 MTU liên kết** (Link MTU)

Đơn vị truyền tải tối đa của một liên kết, tức là kích thước lớn nhất của một gói tin (tính bằng octet) có thể truyền tải được qua một liên kết.

**3.7 MTU của tuyến** (Path MTU)

MTU liên kết nhỏ nhất trong tất cả các MTU liên kết trên một tuyến giữa nút nguồn và nút đích.

CHÚ THÍCH 1: Thuật ngữ MTU của tuyến tương đương với thuật ngữ MTU tuyến nêu tại mục 3.12 trong TCVN 9802-1:2013.

CHÚ THÍCH 2: Thuật ngữ tuyến sử dụng trong Quy chuẩn này tương đương với thuật ngữ đường truyền sử dụng trong TCVN 9802-1:2013.

**3.8 Phát hiện Path MTU**

Quá trình nút IPv6 xác định MTU của tuyến.

**3.9 Lựa chọn địa chỉ mặc định IPv6**

Việc lựa chọn địa chỉ nguồn hay địa chỉ đích sử dụng mặc định để truyền thông tin trong trường hợp có nhiều địa chỉ khả dụng (nhiều địa chỉ trong một giao diện hoặc nhiều hướng đi khác nhau).

**3.10 Tự động cấu hình địa chỉ không giữ trạng thái IPv6**

Kỹ thuật cấu hình địa chỉ cho các host mà không cần cấu hình bằng tay, chỉ yêu cầu cấu hình tối thiểu của các router và không cần máy chủ. Kỹ thuật tự động cấu hình địa chỉ không giữ trạng thái cho phép host tạo ra địa chỉ của host đó bằng cách kết hợp thông tin cục bộ của host (định danh giao diện) và thông tin quảng bá bởi router (tiền tố).

**3.11 Phát hiện đối tượng nghe multicast** (MLD)

Kỹ thuật cho phép router phát hiện các đối tượng nghe multicast (tức là các nút mong muốn nhận gói tin multicast) trên các liên kết gắn trực tiếp với router này và phát hiện những địa chỉ multicast nào mà các nút lân cận này quan tâm.

**3.12 Công nghệ đường hầm**

Công nghệ cho phép gửi các gói tin IP trên các gói tin IP. Ví dụ, đường hầm IPv6 qua IPv4 thực hiện đóng gói các gói tin IPv6 trong các gói tin IPv4 để truyền qua hạ tầng mạng định tuyến IPv4.

**3.13 Thuật ngữ chỉ mức độ yêu cầu**

Các từ khóa "PHẢI", "KHÔNG PHẢI", "BẮT BUỘC", "SẼ", "KHÔNG ĐƯỢC", "NÊN", "KHÔNG NÊN", "KHUYẾN NGHỊ", "KHÔNG KHUYẾN NGHỊ", "CÓ THỂ" và "TÙY CHỌN" trong tài liệu này phải được hiểu như mô tả trong BCP 14 [RFC2119] [RFC8174] khi và chỉ khi, chúng xuất hiện bằng tất cả các chữ hoa, như được hiển thị ở đây.

# Các từ viết tắt sử dụng trong tiêu chuẩn

| **Từ viết tắt** | **Tiếng Anh** | **Tiếng Việt** |
| --- | --- | --- |
| AH | Authentication Header | Tiêu đề xác thực |
| DAD | Duplicate Address Detection | Phát hiện địa chỉ trùng lặp |
| ESP | Encapsulating Security Payload | Đóng gói tải tin bảo mật |
| ICMP | Internet Control Message Protocol | Giao thức bản tin kiểm soát Internet |
| IKE | Internet Key Exchange | Trao đổi khóa Internet |
| MIB | Management Information Base | Cơ sở thông tin quản lý |
| MLD | Multicast Listener Discovery | Phát hiện trình nghe đa hướng |
| MTU | Maximum Transmission Unit | Đơn vị truyền tối đa |
| NA | Neighbor Advertisement | Quảng cáo lân cận |
| NEMA | Non-Broadcast Multi-Access | Đa truy cập không truyền phát quảng bá |
| ND | Neighbor Discovery | Phát hiện lân cận |
| NS | Neighbor Solicitation | Yêu cầu lân cận |
| NUD | Neighbor Unreachability Detection | Phát hiện không thể chia sẻ lân cận |
| PPP | Point-to-Point Protocol | Giao thức điểm - điểm |

# Giới thiệu

Tiêu chuẩn này xác định các yêu cầu đối với các nút IPv6. Với mong muốn rằng IPv6 sẽ được triển khai rộng rãi trên nhiều loại thiết bị và tình huống. Chỉ định yêu cầu các nút IPv6 cho phép triển khai IPv6 có các chức năng và liên kết hoạt động trong một số lượng lớn các tình huống.

RFC 8504 (2019) thay thế cho RFC 6434 (2011) và RFC 4294 (2006).

Tiêu chuẩn này xác định chức năng chung yêu cầu từ cả các máy chủ và bộ định tuyến IPv6. Nhiều nút IPv6 sẽ triển khai các tính năng tùy chọn hoặc bổ sung, nhưng tiêu chuẩn này thu thập và tổng hợp yêu cầu từ các Tài liệu theo vết các Tiêu chuẩn được xuất bản ở nơi khác.

Tiêu chuẩn này cố gắng tránh thảo luận về chi tiết giao thức và tham chiếu tới các RFC cho mục đích này. Tiêu chuẩn này nhằm mục đích tuyên bố về khả năng áp dụng và cung cấp hướng dẫn về thông số kỹ thuật IPv6 cần được thực hiện trong trường hợp chung và các thông số kỹ thuật có thể được quan tâm trong các kịch bản triển khai cụ thể. Tiêu chuẩn này không cập nhật bất kỳ tài liệu giao thức riêng biệt nào của các RFC.

Mặc dù tiêu chuẩn này chỉ ra các thông số kỹ thuật khác nhau, nhưng cần phải lưu ý rằng trong nhiều trường hợp, mức độ chi tiết của một yêu cầu sẽ nhỏ hơn một thông số kỹ thuật riêng biệt, vì nhiều thông số kỹ thuật xác định ghép hợp bởi nhiều phần độc lập, mà một số phần trong số đó có thể là không bắt buộc. Ngoài ra, hầu hết các thông số kỹ thuật xác định cả hai hành vi của máy khách và máy chủ trong cùng một thông số kỹ thuật, trong khi nhiều triển khai sẽ chỉ tập trung vào một trong những vai trò đó.

Tiêu chuẩn này xác định mức tối thiểu của yêu cầu cần thiết cho một thiết bị để cung cấp dịch vụ Internet hữu ích và xem xét trên phạm vi rộng chủng loại thiết bị và các kịch bản triển khai. Bởi vì phạm vi rộng của các kịch bản triển khai, cho nên các yêu cầu tối thiểu được ấn định trong tiêu chuẩn này có thể không đủ cho tất cả các kịch bản triển khai. Hoàn toàn hợp lý (và thực sự được mong đợi) để các hồ sơ khác xác định các yêu cầu bổ sung hoặc nghiêm ngặt hơn cho các môi trường sử dụng và triển khai. Ví dụ, tiêu chuẩn này không bắt buộc tất cả các máy khách hỗ trợ DHCP, nhưng một số kịch bản triển khai có thể được cho là phù hợp để đưa ra yêu cầu như vậy. Theo một ví dụ khác, NIST đã xác định hồ sơ cho các yêu cầu chuyên biệt đối với IPv6 trong môi trường mục tiêu ([USGv6]).

Vì không phải lúc nào người triển khai cũng có thể biết chính xác cách sử dụng IPv6 trong một nút, một yêu cầu quan trọng hơn đối với các nút IPv6 đó là chúng nên tuân thủ Nguyên tắc chắc chắn của Jon Postel “Bảo toàn trong những gì bạn làm, hào phóng trong những gì bạn chấp nhận từ những người khác [RFC793]”.

# Tầng IP con

Một nút IPv6 PHẢI bao gồm hỗ trợ cho một hoặc nhiều thông số kỹ thuật tầng liên kết IPv6. Các thông số kỹ thuật của tầng liên kết triển khai nên bao gồm sự phụ thuộc vào các tầng liên kết nào được hỗ trợ bởi phần cứng có sẵn trên hệ thống. Một nút IPv6 phù hợp có thể hỗ trợ IPv6 trên một số giao diện của nó chứ không phải các giao diện khác.

Do IPv6 được chạy trên các công nghệ Lớp 2 mới, cho nên dự kiến ​​các thông số kỹ thuật mới sẽ được ban hành. Sau đây liệt kê một số công nghệ Lớp 2 mà thông số kỹ thuật IPv6 đã được phát triển. Nó chỉ cung cấp cho mục đích thông tin và có thể không đầy đủ.

- Truyền các gói IPv6 qua mạng Ethernet [RFC2464].

- Truyền các gói IPv6 qua thông số kỹ thuật mạng chuyển tiếp khung [RFC2590].

- Truyền các gói IPv6 qua mạng IEEE 1394 [RFC3146].

- Truyền IPv6, IPv4 và gói giao thức phân giải địa chỉ (ARP) qua kênh sợi quang [RFC4338].

- Truyền các gói IPv6 qua mạng IEEE 802.15.4 [RFC4944].

- Truyền IPv6 qua tầng con hội tụ IPv6 qua Mạng IEEE 802.16 [RFC5121].

- IP phiên bản 6 qua PPP [RFC5072].

Ngoài các tầng liên kết vật lý truyền thống, cũng có thể tạo đường hầm IPv6 qua các giao thức khác. Các ví dụ gồm:

- Teredo tạo đường hầm IPv6 qua UDP thông qua dịch chuyển địa chỉ mạng (NAT) [RFC4380].

- Các cơ chế chuyển đổi cơ bản cho máy chủ và bộ định tuyến IPv6 (xem Phần 3 của [RFC4213]).

# Tầng IP

## Giao thức Internet phiên bản 6 – RFC 8200

Giao thức Internet phiên bản 6 được chỉ định trong [RFC8200]. Thông số kỹ thuật này PHẢI được hỗ trợ.

Thiết bị nút PHẢI tuân theo các quy tắc truyền gói trong RFC 8200.

Tất cả các triển khai IPv6 thích ứng PHẢI có khả năng gửi và nhận các gói IPv6; chức năng chuyển tiếp CÓ THỂ được hỗ trợ. Các thiết bị nút PHẢI luôn có thể gửi, nhận và xử lý các tiêu đề đoạn.

Các nút IPv6 KHÔNG ĐƯỢC tạo các đoạn chồng chéo. Ngoài ra, khi tập hợp lại một gói dữ liệu IPv6, nếu một hoặc nhiều đoạn cấu thành của nó được xác định là một đoạn chồng chéo, thì toàn bộ gói dữ liệu (và bất kỳ đoạn cấu thành) PHẢI bị loại bỏ một cách lặng lẽ. Xem [RFC5722] để biết thêm thông tin.

Theo khuyến nghị trong [RFC8021], các thiết bị nút KHÔNG ĐƯỢC tạo ra các phân mảnh, tức là, trong đó phân mảnh là toàn bộ gói dữ liệu. Theo [RFC6946], nếu một nút nhận đang lắp ráp lại một gói dữ liệu gặp phải một phân mảnh, thì nó sẽ được xử lý như một gói được lắp ráp lại hoàn toàn và bất kỳ phân mảnh nào khác khớp với gói này sẽ được xử lý độc lập.

Để giảm thiểu một loạt các cuộc tấn công tiềm ẩn, các nút NÊN tránh sử dụng các giá trị nhận dạng phân mảnh có thể dự đoán được trong các tiêu đề phân mảnh, như đã thảo luận trong [RFC7739].

Tất cả các thiết bị nút NÊN hỗ trợ cài đặt và sử dụng trường nhãn luồng IPv6 như được định nghĩa trong thông số kỹ thuật nhãn luồng IPv6 [RFC6437]. Các nút chuyển tiếp như bộ định tuyến và bộ phân phối tải KHÔNG PHẢI chỉ phụ thuộc vào các giá trị nhãn luồng được phân phối đồng nhất. KHUYẾN NGHỊ rằng các máy chủ nguồn hỗ trợ nhãn luồng bằng cách đặt trường nhãn luồng cho tất cả các gói của một luồng nhất định thành cùng một giá trị được chọn từ một giá trị gần đúng đến một phân phối đồng nhất rời rạc.

## Hỗ trợ cho các tiêu đề mở rộng IPv6

RFC 8200 chỉ định các tiêu đề mở rộng và xử lý các tiêu đề này.

Các tiêu đề mở rộng (ngoại trừ tiêu đề tùy chọn chặng tới chặng) không được xử lý, chèn hoặc xóa bởi bất kỳ nút nào dọc theo đường phân phối của gói, cho đến khi gói đến nút (hoặc từng nhóm nút, trong trường hợp đa hướng) được xác định trong trường địa chỉ đích của tiêu đề IPv6.

Bất kỳ tiêu đề hoặc tùy chọn mở rộng không được công nhận PHẢI được xử lý như đã mô tả trong RFC 8200. Lưu ý rằng trong đó Phần 4 của RFC 8200 đề cập đến hành động được thực hiện khi giá trị tiêu đề tiếp theo trong tiêu đề hiện tại không được công nhận bởi một nút nhận dạng, hành động đó áp dụng cho dù giá trị là tiêu đề mở rộng không được công nhận hoặc giao thức tầng trên (ULP) không được công nhận.

Một thiết bị nút IPv6 PHẢI có khả năng xử lý các tiêu đề mở rộng này. Ngoại trừ là loại tiêu đề định tuyến 0 (RH0), đã không được tán thành bởi [RFC5095] do liên quan đến bảo mật và PHẢI được coi là loại định tuyến không được công nhận.

Hơn nữa, [RFC7045] bổ sung các yêu cầu cụ thể đối với việc xử lý các tiêu đề mở rộng, cụ thể là bất kỳ nút chuyển tiếp nào dọc theo đường dẫn của gói IPv6, chuyển tiếp gói tin vì bất kỳ lý do gì, NÊN làm như vậy bất kể có sự hiện diện của bất kỳ tiêu đề mở rộng nào.

Theo RFC 8200, khi một nút phân đoạn một gói dữ liệu IPv6, nó PHẢI bao gồm toàn bộ chuỗi tiêu đề IPv6 trong phân mảnh đầu tiên. Các tiêu đề mỗi phân mảnh PHẢI bao gồm tiêu đề IPv6 cộng với bất kỳ tiêu đề mở rộng nào PHẢI được xử lý bởi các nút trên đường đến đích, đó là tất cả các tiêu đề ở trên và gồm cả tiêu đề định tuyến nếu có, nếu không có tiêu đề tùy chọn từng chặng, thì không có tiêu đề mở rộng. Khi lắp ráp lại, nếu phân mảnh đầu tiên không bao gồm tất cả các tiêu đề thông qua một tiêu đề lớp trên, thì phân mảnh đó NÊN bị loại bỏ và vấn đề tham số ICMP, Mã 3, thông báo NÊN được gửi đến nguồn của phân mảnh, với trường con trỏ được đặt về không. Xem [RFC7112] để thảo luận về lý do tránh các chuỗi tiêu đề IPv6 mở rộng quá khổ.

Khuyến nghị không nên xác định tiêu đề mở rộng IPv6 mới, trừ khi không có tiêu đề mở rộng IPv6 hiện có nào có thể được sử dụng bằng cách chỉ định một tùy chọn mới cho tiêu đề mở rộng IPv6 đó. Đề xuất chỉ định một tiêu đề mở rộng IPv6 mới PHẢI bao gồm giải thích kỹ thuật chi tiết về lý do tại sao tiêu đề mở rộng IPv6 hiện có không thể được sử dụng cho chức năng mới mong muốn, và trong những trường hợp như vậy, cần phải tuân theo định dạng được mô tả trong Phần 8 của RFC 8200 để đọc thêm thông tin cơ bản về chủ đề này, xem [RFC6564].

## Bảo vệ nút khỏi các tùy chọn tiêu đề mở rộng quá mức

Theo RFC 8200, các máy chủ kết cuối dự kiến xử lý tất cả các tiêu đề mở rộng, tùy chọn đích và tùy chọn từng chặng trong một gói. Do giới hạn duy nhất về số lượng và kích thước của các tiêu đề mở rộng là MTU, nên việc xử lý các gói nhận được có thể là đáng kể. Cũng có thể hình dung rằng một chuỗi dài các tiêu đề mở rộng có thể được sử dụng như một hình thức tấn công từ chối dịch vụ. Theo đó, một máy chủ có thể đặt giới hạn về số lượng và kích thước của các tiêu đề mở rộng và các tùy chọn mà nó sẵn sàng xử lý.

Một máy chủ CÓ THỂ giới hạn số lượng tùy chọn PAD1 liên tiếp trong các tùy chọn đích hoặc các tùy chọn từng chặng tới 7. Trong trường hợp này, nếu có nhiều hơn 7 tùy chọn PAD1 liên tiếp, thì gói tin CÓ THỂ bị loại bỏ lặng lẽ. Cơ sở lý luận là nếu yêu cầu có đệm từ 8 bytes trở lên, thì tùy chọn PADN NÊN được sử dụng.

Một máy chủ CÓ THỂ giới hạn số byte trong tùy chọn một PADN nhỏ hơn 8. Trong trường hợp như vậy, nếu có một tùy chọn PADN có độ dài lớn hơn 7, thì gói tin NÊN bị loại bỏ lặng lẽ. Cơ sở lý luận của hướng dẫn này là mục đích của đệm là để đồng chỉnh và 8 bytes là đồng chỉnh tối đa được sử dụng trong IPv6.

Một máy chủ CÓ THỂ không cho phép các tùy chọn không biết trong các tùy chọn đích hoặc các tùy chọn từng chặng. Điều này NÊN có thể được định cấu hình trong đó mặc định là chấp nhận các tùy chọn không biết và xử lý chúng theo [RFC8200]. Nếu một gói tin có các tùy chọn không biết được thu nhận và máy chủ được cấu hình để không cho phép chúng, thì gói tin NÊN bị loại bỏ lặng lẽ.

Một máy chủ CÓ THỂ áp đặt giới hạn về số lượng tối đa các tùy chọn không đệm được phép trong các tùy chọn đích và tiêu đề mở rộng từng chặng. Nếu tính năng này được hỗ trợ, thì số lượng tối đa NÊN có thể định cấu hình, và giá trị mặc định NÊN được đặt thành 8. Các giới hạn cho các tùy chọn đích và tùy chọn từng chặng có thể được định cấu hình riêng biệt. Nếu một gói được thu nhận và số lượng tùy chọn đích hoặc từng chặng vượt quá giới hạn, thì gói đó NÊN bị loại bỏ lặng lẽ.

Một máy chủ CÓ THỂ áp đặt giới hạn về độ dài tối đa của các tiêu đề mở rộng tùy chọn đích hoặc tùy chọn từng chặng. Giá trị này NÊN có thể định cấu hình, và mặc định là chấp nhận các tùy chọn có độ dài bất kỳ. Nếu một gói được thu nhận và độ dài của tiêu đề mở rộng tùy chọn đích hoặc từng chặng vượt quá giới hạn độ dài, thì gói NÊN bị loại bỏ lặng lẽ.

## Phát hiện nút mạng lân cận cho IPv6 - RFC 4861

Phát hiện cận được định nghĩa trong [RFC4861]; định nghĩa đã được cập nhật bởi [RFC5942]. Phát hiện lân cận PHẢI được hỗ trợ với các lưu ý ngoại lệ dưới đây. Trạng thái RFC 4861:

- Trừ khi được chỉ định khác (trong một tài liệu bao gồm IP hoạt động trên một loại liên kết cụ thể), tiêu chuẩn này áp dụng cho tất cả các loại liên kết. Tuy nhiên, bởi vì ND sử dụng tầng liên kết đa hướng cho một số dịch vụ của nó, cho nên có thể trên một số loại liên kết (ví dụ: các liên kết đa truy nhập không phát quảng bá (NBMA)), các giao thức hoặc cơ chế thay thế để triển khai các dịch vụ đó sẽ được chỉ định (trong tài liệu thích hợp đề cập đến hoạt động của IP trên một loại liên kết cụ thể). Các dịch vụ được mô tả trong tiêu chuẩn này không phụ thuộc trực tiếp vào truyền phát đa hướng, chẳng hạn như chuyển hướng, xác định chặng tiếp theo, phát hiện không thể kết nối lân cận, v.v…, dự kiến ​​sẽ được cung cấp như quy định trong tiêu chuẩn này. Chi tiết về cách một người sử dụng ND trên các liên kết NBMA được đề cập trong [RFC2491].

Một số phân tích chi tiết của phát hiện lân cận như sau:

- Phát hiện bộ định tuyến là cách các máy chủ định vị các bộ định tuyến nằm trên một liên kết đính kèm. Các máy chủ PHẢI hỗ trợ chức năng phát hiện bộ định tuyến.

- Phát hiện tiền tố là cách các máy chủ phát hiện tập hợp các tiền tố địa chỉ để xác định đích nào là liên kết trên cho một liên kết được đính kèm. Máy chủ PHẢI hỗ trợ phát hiện tiền tố.

- Các máy chủ cũng PHẢI triển khai phát hiện không thể kết nối lân cận (NUD) cho tất cả các đường dẫn giữa máy chủ và các nút lân cận. NUD không bắt buộc đối với đường dẫn giữa các bộ định tuyến. Tuy nhiên, tất cả các nút PHẢI trả lời các bản tin yêu cầu lân cận (NS) đơn hướng.

- [RFC7048] thảo luận về NUD, trong những trường hợp cụ thể khi nó ứng xử quá nôn nóng. Nó tuyên bố rằng nếu một nút truyền nhiều hơn một số gói nhất định, thì nó NÊN sử dụng bộ đếm thời gian truyền lùi lại theo hàm mũ, lên đến một điểm ngưỡng nhất định.

Các máy chủ PHẢI hỗ trợ việc gửi các yêu cầu định tuyến và nhận các quảng cáo định tuyến (RA). Khả năng hiểu các tùy chọn RA riêng lẻ phụ thuộc vào việc hỗ trợ chức năng sử dụng tùy chọn cụ thể.

[RFC7559] thảo luận về khả năng phục hồi mất gói đối với các yêu cầu định tuyến và yêu cầu các nút PHẢI sử dụng một thuật toán dự phòng theo hàm mũ cụ thể để truyền lại các yêu cầu định tuyến.

Tất cả các nút PHẢI hỗ trợ gửi và nhận các bản tin yêu cầu lân cận (NS) và quảng cáo lân cận (NA). Các bản tin NS và NA được yêu cầu cho phát hiện địa chỉ trùng lặp (DAD).

Các máy chủ NÊN hỗ trợ việc xử lý chức năng chuyển hướng. Các bộ định tuyến PHẢI hỗ trợ gửi các chuyển hướng, mặc dù không nhất thiết cho mọi gói riêng lẻ (ví dụ: do giới hạn tốc độ). Chuyển hướng chỉ hữu ích trên các mạng hỗ trợ máy chủ. Trong các mạng lõi bị chi phối bởi định tuyến, chuyển hướng thường bị vô hiệu hóa. Việc gửi các chuyển hướng NÊN bị vô hiệu hóa theo mặc định trên các bộ định tuyến được thiết kế để triển khai trên các mạng lõi. Chúng CÓ THỂ được bật theo mặc định trên các bộ định tuyến nhằm hỗ trợ các máy chủ trên các mạng biên.

Như được chỉ định trong [RFC6980], các nút KHÔNG ĐƯỢC sử dụng phân đoạn IPv6 để gửi bất kỳ bản tin phát hiện lân cận và phát hiện lân cận bảo mật nào sau đây: Yêu cầu lân cận, quảng cáo lân cận, yêu cầu định tuyến, quảng cáo định tuyến, chuyển hướng, hoặc yêu cầu đường dẫn chứng nhận. Các nút PHẢI im lặng bỏ qua bất kỳ bản tin nào trong số này khi nhận được nếu bị phân mảnh. Xem RFC 6980 để biết chi tiết và thúc đẩy.

"Chia sẻ tải từ máy chủ đến bộ định tuyến IPv6" [RFC4311] bao gồm các khuyến nghị bổ sung về cách lựa chọn từ một bộ bộ định tuyến có sẵn. [RFC4311] NÊN được hỗ trợ.

## Phát hiện lân cận bảo mật (SEND) - RFC 3971

SEND [RFC3971] và địa chỉ được tạo ra bằng mật mã hóa (CGA) [RFC3972] cung cấp một cách để bảo mật trao đổi bản tin phát hiện lân cận. SEND có khả năng giải quyết một số loại tấn công giả mạo nhất định, nhưng nó không cung cấp biện pháp bảo vệ cụ thể đối với các mối đe dọa từ những kẻ tấn công ngoài liên kết.

Có tương đối ít việc triển khai SEND trong các hệ điều hành và nền tảng phổ biến kể từ khi nó được công bố năm 2005; do đó, cho đến nay kinh nghiệm triển khai vẫn còn rất hạn chế.

Tại thời điểm này, hỗ trợ cho SEND được coi là tùy chọn. Do sự phức tạp trong việc triển khai SEND và sự cung cấp nặng nề của nó, nên việc triển khai nó chỉ có thể được xem xét khi các nút đang hoạt động trong một môi trường bảo mật đặc biệt nghiêm ngặt.

## Tùy chọn cờ quảng cáo bộ định tuyến IPv6 - RFC 5175

Các quảng cáo bộ định tuyến bao gồm một trường 8-bit cờ quảng cáo bộ định tuyến một-bit. Tùy chọn cờ quảng cáo bộ định tuyến mở rộng số bit cờ có sẵn thêm 48 bit. Tại thời điểm công bố tiêu chuẩn này, 6 trong số 8 cờ bit đơn ban đầu đã được gán, trong khi 2 cờ vẫn có sẵn để gán trong tương lai. Không có cờ nào được xác định để sử dụng tùy chọn mới; do đó, nói một cách chính xác, không có yêu cầu nào để thực hiện tùy chọn hiện nay. Tuy nhiên, các triển khai có thể chuyển các tùy chọn không được công nhận cho một thực thể cấp cao hơn có thể hiểu được chúng (ví dụ: quy trình cấp người dùng sử dụng cơ sở "ổ cắm thô") CÓ THỂ thực hiện các bước để xử lý tùy chọn với dự đoán sử dụng trong tương lai.

## Phát hiện đường dẫn MTU và kích cỡ gói

### Phát hiện đường dẫn MTU – RFC 8201

"Phát hiện đường dẫn MTU đối với IP phiên bản 6" [RFC8201] NÊN được hỗ trợ từ [RFC8200]:

- Khuyến nghị rằng các nút IPv6 nên triển khai phát hiện đường dẫn MTU [RFC8201], để phát hiện và tận dụng các đường dẫn MTU lớn hơn 1280 octet. Tuy nhiên, việc triển khai IPv6 tối thiểu (ví dụ: trong một ROM khởi động) có thể chỉ tự hạn chế gửi các gói không lớn hơn 1280 octet và bỏ qua việc triển khai phát hiện đường dẫn MTU.

Các quy tắc trong [RFC8200] và [RFC5722] PHẢI tuân theo để phân mảnh và lắp ráp lại gói.

Như được mô tả trong RFC 8201, các nút triển khai phát hiện đường dẫn MTU và gửi các gói lớn hơn liên kết tối thiểu IPv6 MTU dễ có vấn đề kết nối nếu các bản tin ICMPv6 bị chặn hoặc không được truyền. Ví dụ: điều này sẽ dẫn đến kết nối hoàn thành bắt tay ba chiều TCP một cách chính xác nhưng rồi bị treo khi dữ liệu được truyền. Trạng thái này được gọi là kết nối lỗ đen [RFC2923]. Phát hiện đường dẫn MTU dựa trên gói quá lớn (PTB) ICMPv6 để xác định đường dẫn MTU (và do đó các đường dẫn này KHÔNG PHẢI được lọc, theo khuyến nghị trong [RFC4890]).

Giải pháp thay thế cho phát hiện đường dẫn MTU được xác định trong RFC 8201 có thể được tìm thấy trong [RFC4821], giải pháp này xác định một phương pháp phát hiện đường dẫn MTU lớp đóng gói (PLPMTUD) được thiết kế để sử dụng trên các đường dẫn nơi mà việc phân phối bản tin ICMPv6 tới máy chủ không được đảm bảo.

### Xem xét MTU tối thiểu

Mặc dù MTU liên kết IPv6 có thể được đặt thành 1280 byte, nhưng khuyến nghị rằng đối với IPv6 UDP nói riêng, bao gồm hoạt động DNS, nút gửi sử dụng MTU lớn nếu chúng có thể, để tránh rớt gói do phân mảnh vô cớ.

## ICMP cho giao thức Internet phiên bản 6 (IPv6) - RFC 4443

ICMPv6 [RFC4443] PHẢI được hỗ trợ. "ICMP được mở rộng để hỗ trợ bản tin nhiều phần" [RFC4884] CÓ THỂ được hỗ trợ.

## Ưu tiên bộ định tuyến mặc định và các bộ định tuyến đặc trưng hơn - RFC 4191

"Ưu tiên bộ định tuyến mặc định và các bộ định tuyến đặc trưng hơn" [RFC4191] cung cấp hỗ trợ cho các nút được gắn với nhiều mạng (khác nhau), mỗi mạng cung cấp các bộ định tuyến tự quảng cáo như bộ định tuyến mặc định thông qua quảng cáo định tuyến. Trong một số kịch bản, một bộ định tuyến có thể cung cấp kết nối đến các đích mà bộ định tuyến kia không cung cấp, và việc lựa chọn bộ định tuyến mặc định "sai" có thể dẫn đến lỗi khả năng truy cập. Để giải quyết tình huống này, các nút IPv6 PHẢI triển khai [RFC4191] và NÊN triển khai vai trò máy chủ loại C được xác định trong RFC 4191.

## Lựa chọn bộ định tuyến chặng đầu tiên - RFC 8028

Trong các kịch bản đa mạng, ở đó máy chủ có nhiều hơn một tiền tố, mỗi tiền tố được phân bổ bởi một mạng luồng lên được giả định để triển khai lọc xâm nhập BCP 38, máy chủ có thể có nhiều bộ định tuyến để lựa chọn.

Các máy chủ có thể được triển khai trong môi trường đa mạng như vậy NÊN tuân theo hướng dẫn được đưa ra trong [RFC8028].

## Phát hiện lắng nghe truyền phát đa hướng (MLD) cho IPv6 – RFC 3810

Các nút cần tham gia nhóm truyền phát đa hướng PHẢI hỗ trợ MLDv2 [RFC3810]. MLD là cần thiết bởi bất kỳ nút nào dự kiến ​​sẽ nhận và xử lý lưu lượng truyền phát đa hướng; đặc biệt, MLDv2 được yêu cầu để hỗ trợ cho truyền phát đa hướng nguồn đặc trưng (SSM) theo [RFC4607].

Các phiên bản trước của thông số kỹ thuật này chỉ yêu cầu MLDv1 [RFC2710] được triển khai trên tất cả các nút. Vì sự tham gia của bất kỳ nút MLDv1 duy nhất nào trên một liên kết yêu cầu tất cả các nút khác trên liên kết phải hoạt động ở chế độ tương thích phiên bản 1, yêu cầu hỗ trợ MLDv2 trên tất cả các nút đã được cập nhật thành PHẢI. Hơn nữa, SSM hiện là phương pháp phân phối truyền phát đa hướng được ưa thích hơn là nguồn truyền phát đa hướng bất kỳ (ASM).

Lưu ý rằng Phát hiện lân cận (như được sử dụng trên hầu hết các loại liên kết - xem 7.4) tùy thuộc vào truyền phát đa hướng và yêu cầu các nút tham gia nút được yêu cầu địa chỉ truyền phát đa hướng.

## Thông báo tắc nghẽn rõ ràng (ECN) - RFC 3168

Một bộ định tuyến nhận biết ECN đặt một nhãn trong tiêu đề IP để báo hiệu tắc nghẽn sắp xảy ra, thay vì làm rớt một gói tin. Bộ thu gói tin hồi đáp lại chỉ báo tắc nghẽn tới bộ gửi, sau đó có thể giảm tốc độ truyền của nó nếu như nó phát hiện một gói tin bị rớt.

Các nút NÊN hỗ trợ ECN [RFC3168] bằng cách triển khai giao diện cho tầng trên để truy cập và bằng cách đặt các bit ECN trong tiêu đề IP. Các lợi ích của việc sử dụng ECN được công bố trong [RFC8087].

# Định địa chỉ và cấu hình địa chỉ

## Kiến trúc định địa chỉ IP phiên bản 6 – RFC 4291

Kiến trúc định địa chỉ IPv6 [RFC4291] PHẢI được hỗ trợ.

Kiến trúc địa chỉ IPv6 hiện tại dựa trên ranh giới 64 bits cho các tiền tố mạng con. Lý do đằng sau quyết định này được công bố trong [RFC7421].

Việc triển khai cũng PHẢI hỗ trợ các bản cập nhật cờ truyền phát đa hướng công bố trong [RFC7371].

## Khuyến nghị tính khả dụng của địa chỉ máy chủ

Máy chủ có thể được cấu hình địa chỉ thông qua nhiều phương pháp, bao gồm tự động cấu hình địa chỉ phi trạng thái (SLAAC), DHCPv6, hoặc cấu hình thủ công.

[RFC7934] khuyến nghị rằng các mạng cung cấp các máy chủ kết cuối có mục đích chung với nhiều địa chỉ IPv6 toàn cầu khi chúng gắn kèm, và nó mô tả các lợi ích cũng như các tùy chọn để làm như vậy. Bộ định tuyến NÊN hỗ trợ [RFC7934] để gán nhiều địa chỉ cho một máy chủ. Một máy chủ NÊN hỗ trợ gán nhiều địa chỉ như được mô tả trong [RFC7934].

Các thiết bị nút NÊN hỗ trợ khả năng được gán một tiền tố cho mỗi máy chủ như được công bố trong [RFC8273]. Cách tiếp cận như vậy có thể đưa ra cải thiện cách ly máy chủ và nâng cao quản lý thuê bao trên các phân đoạn mạng được chia sẻ.

## Tự động cấu hình địa chỉ phi trạng thái IPv6 – RFC 4862

Các máy chủ PHẢI hỗ trợ tự động cấu hình địa chỉ phi trạng thái IPv6. Điều đó được KHUYẾN CÁO như đã mô tả trong [RFC8064], rằng trừ khi có một yêu cầu cụ thể đối với địa chỉ kiểm soát truy cập phương tiện (MAC) được nhúng vào một mã định danh giao diện (IID), các nút sẽ tuân theo quy trình trong [RFC7217] để tạo ra các địa chỉ dựa trên SLAAC, thay vì sử dụng [RFC4862]. Các địa chỉ được tạo ra sử dụng phương pháp được mô tả trong [RFC7217] sẽ giống nhau bất cứ khi nào một thiết bị nhất định xuất hiện (xuất hiện lại) trên cùng một mạng con (với một tiền tố IPv6 cụ thể), nhưng IID sẽ khác nhau trên mỗi mạng con tạm trú.

Các nút ở đó các bộ định tuyến PHẢI có thể tạo ra địa chỉ liên kết cục bộ như được mô tả trong [RFC4862].

Từ RFC 4862: Quy trình tự động định cấu hình được chỉ định trong tiêu chuẩn này chỉ áp dụng cho các máy chủ chứ không phải các bộ định tuyến. Vì tự động cấu hình máy chủ sử dụng thông tin được quảng cáo bởi các bộ định tuyến, nên các bộ định tuyến sẽ cần được cấu hình bằng một số phương tiện khác. Tuy nhiên, dự kiến ​​rằng các bộ định tuyến sẽ tạo ra các địa chỉ liên kết cục bộ sử dụng cơ chế được mô tả trong tiêu chuẩn này. Ngoài ra, các bộ định tuyến được dự kiến hoàn thành thông qua quy trình phát hiện địa chỉ trùng lặp được mô tả trong tiêu chuẩn này trên tất cả các địa chỉ trước khi gán chúng vào một giao diện.

Tất cả các nút PHẢI triển khai phát hiện địa chỉ trùng lặp. Trích dẫn từ 7.4 của RFC 4862:

- Phát hiện địa chỉ trùng lặp PHẢI được thực hiện trên tất cả các địa chỉ truyền phát đơn hướng trước khi gán chúng vào một giao diện, bất kể chúng có được thông qua cấu hình tự động phi trạng thái, DHCPv6, hay cấu hình thủ công, với các ngoại lệ sau [được lưu ý trong đó].

- "Phát hiện địa chỉ trùng lặp (DAD) tối ưu cho IPv6" [RFC4429] chỉ định một cơ chế để giảm độ trễ liên quan đến tạo địa chỉ thông qua tự động định cấu hình địa chỉ phi trạng thái [RFC4862]. RFC 4429 được phát triển cùng với IPv6 di động nhằm giảm thời gian cần thiết để lấy và cấu hình địa chỉ khi các thiết bị nhanh chóng di chuyển từ mạng này sang mạng khác, và nó mong muốn giảm thiểu trễ chuyển dịch. Đối với các thiết bị mục tiêu chung, RFC 4429 vẫn là tùy chọn tại thời điểm này.

[RFC7527] thảo luận về DAD nâng cao và mô tả một thuật toán tự động hóa phát hiện các bản tin ND IPv6 lặp lại được sử dụng bởi DAD. Các nút NÊN thực hiện hành vi này tại nơi phát hiện như vậy là có lợi.

## Mở rộng quyền riêng tư cho cấu hình địa chỉ trong IPv6 - RFC 4941

Một nút sử dụng tự động cấu hình địa chỉ phi trạng thái [RFC4862] để tạo dạng địa chỉ IPv6 duy nhất trên toàn cầu ở đó sử dụng địa chỉ MAC của nó để tạo ra IID sẽ thấy rằng IID vẫn giữ nguyên trên bất kỳ mạng tạm trú nào, ngay cả khi phần tiền tố mạng thay đổi. Do đó, có thể xảy ra một thiết bị của bên thứ ba theo vết các hoạt động của thiết bị nút mà chúng giao tiếp với nhau, khi nút đó di chuyển xung quanh mạng. Mở rộng quyền riêng tư cho tự động cấu hình địa chỉ phi trạng thái [RFC4941] giải quyết mối lo ngại này bằng cách cho phép các nút cấu hình bổ sung địa chỉ tạm thời, nơi IID được tạo ra ngẫu nhiên một cách hiệu quả. Địa chỉ riêng tư sau đó được sử dụng làm địa chỉ nguồn cho các giao tiếp mới được khởi xướng bởi thiết bị nút.

Các vấn đề chung liên quan đến quyền riêng tư đối với địa chỉ IPv6 được thảo luận trong [RFC7721].

RFC 4941 NÊN được hỗ trợ. Trong một số trường hợp, chẳng hạn như máy chủ chuyên dụng trong một trung tâm dữ liệu, nó cung cấp lợi ích hạn chế hoặc không, hoặc nó có thể làm phức tạp cho việc quản lý mạng. Do đó, các thiết bị thực thi thông số kỹ thuật này PHẢI cung cấp cách thức rõ ràng đối với người dùng cuối để có thể được phép hoặc không được phép sử dụng các địa chỉ tạm thời như vậy.

Lưu ý rằng RFC 4941 có thể được sử dụng độc lập với SLAAC truyền thống hoặc sự độc lập của SLAAC dựa trên RFC 7217.

Những triển khai RFC 4941 nên biết rằng các địa chỉ nhất định đã được đăng ký trước và không nên được lựa chọn để sử dụng làm địa chỉ tạm thời. Tham khảo "Các nhận dạng giao diện IPv6 dành riêng" [RFC5453] để biết thêm chi tiết.

## Tự động định cấu hình địa chỉ trạng thái (DHCPv6) - RFC 3315

DHCPv6 [RFC3315] có thể được sử dụng để lấy và cấu hình các địa chỉ. Nói chung, một mạng có thể cung cấp cấu hình địa chỉ thông qua SLAAC, DHCPv6 hoặc cả hai. Sẽ có nhiều mô hình triển khai IPv6 và sự khác biệt trong các yêu cầu gán địa chỉ, một số có thể yêu cầu DHCPv6 để gán địa chỉ trạng thái. Do đó, tất cả các máy chủ NÊN thực hiện cấu hình địa chỉ thông qua DHCPv6.

Trong trường hợp không có bản tin quảng cáo bộ định tuyến được quan sát, các nút IPv6 CÓ THỂ khởi tạo DHCP để lấy địa chỉ IPv6 và thông tin cấu hình khác, như được mô tả trong Phần 5.5.2 của [RFC4862].

Trường hợp các thiết bị có vẻ thích hợp với người dùng và được gắn vào nhiều mạng tạm trú, các hồ sơ ẩn danh máy khách DHCPv6 NÊN được hỗ trợ như mô tả trong [RFC7844] để giảm thiểu tiết lộ thông tin nhận dạng. Phần 5 của RFC 7844 mô tả các cân nhắc hoạt động khi sử dụng các hồ sơ ẩn danh như vậy.

## Lựa chọn địa chỉ mặc định cho IPv6 - RFC 6724

Các nút IPv6 luôn có nhiều địa chỉ được cấu hình đồng thời và do đó sẽ cần lựa chọn địa chỉ nào để sử dụng cho các giao tiếp nào. PHẢI thực hiện các quy tắc được chỉ định trong lựa chọn địa chỉ mặc định cho tài liệu IPv6 [RFC6724]. [RFC8028] cập nhật quy tắc 5.5 từ [RFC6724]; khi triển khai NÊN thực hiện quy tắc này.

# Hệ thống tên miền (DNS)

DNS được mô tả trong [RFC1034], [RFC1035], [RFC3363] và [RFC3596]. Không phải tất cả các nút sẽ cần phải giải quyết các tên; những tên đó sẽ không bao giờ cần phân giải, các tên DNS không cần triển khai chức năng phân giải. Tuy nhiên, khả năng phân giải tên là một năng lực của cơ sở hạ tầng cơ bản mà các ứng dụng dựa vào, và hầu hết các nút sẽ cần cung cấp hỗ trợ. Tất cả các nút NÊN triển khai chức năng [RFC1034] phân giải gốc, như trong Phần 5.3.1 của [RFC1034], với sự hỗ trợ cho:

- Bản ghi tài nguyên loại AAA [RFC3596];

- Đảo ngược địa chỉ trong ip6.arpa bằng cách sử dụng bản ghi PTR [RFC3596]; và

- Cơ chế mở rộng cho DNS (EDNS (0)) [RFC6891] để cho phép kích cỡ gói DNS lớn hơn 512 octet.

Các nút đó được KHUYẾN NGHỊ để hỗ trợ các mở rộng bảo mật DNS [RFC4033] [RFC4034] [RFC4035].

Bản ghi tài nguyên A6 [RFC2874] được phân loại là lịch sử theo [RFC6563]. Chúng được xác định với các trạng thái thử nghiệm trong [RFC3363].

# Định cấu hình thông tin không địa chỉ

## DHCP cho thông tin cấu hình khác

DHCP [RFC3315] chỉ định một cơ chế để các nút IPv6 lấy thông tin cấu hình địa chỉ (xem 8.5) và lấy thêm cấu hình (không địa chỉ). Nếu một máy chủ triển khai hỗ trợ các ứng dụng hoặc các giao thức khác yêu cầu cấu hình chỉ khả dụng qua DHCP, thì các máy chủ NÊN triển khai DHCP. Đối với các thiết bị chuyên dụng không cần cấu hình như vậy, DHCP có thể không cần thiết.

Một nút IPv6 có thể sử dụng tập hợp con của DHCP (được mô tả trong [RFC3736]) để lấy thông tin cấu hình khác.

Nếu một nút IPv6 triển khai DHCP, nó PHẢI triển khai các tùy chọn DNS [RFC3646] vì hầu hết các triển khai mong muốn rằng các tùy chọn này là khả dụng.

## Quảng cáo bộ định tuyến và cổng mặc định

Không có tùy chọn cổng DHCPv6 được xác định.

Các nút sử dụng giao thức cấu hình máy chủ động cho IPv6 (DHCPv6) mong muốn xác định thông tin định tuyến mặc định và thông tin tiền tố trên liên kết từ các quảng cáo bộ định tuyến đã nhận.

## Tùy chọn quảng cáo bộ định tuyến IPv6 cho cấu hình DNS - RFC 8106

Các tùy chọn quảng cáo bộ định tuyến có lịch sử chỉ giới hạn với những tùy chọn quan trọng đối với chức năng IPv6 cơ bản. Ban đầu, cấu hình DNS không được bao gồm một tùy chọn RA, và DHCP được khuyến cáo cách lấy thông tin cấu hình DNS. Theo thời gian, ý tưởng xoay quanh tùy chọn như vậy đã được tiến triển. Đến nay thừa nhận chung rằng một số nút có thể có chức năng đầy đủ mà không cần truy cập vào giải quyết DNS đang hoạt động; do đó, một tài liệu theo vết tiêu chuẩn đã được xuất bản để cung cấp khả năng này [RFC8106].

Những triển khai PHẢI bao gồm hỗ trợ cho tùy chọn RA DNS [RFC8106].

## Các tùy chọn DHCP so với tùy chọn quảng cáo bộ định tuyến cho cấu hình máy chủ

Trong IPv6, có hai cơ chế giao thức chính để truyền thông tin cấu hình đến máy chủ: các RA và DHCP. Các tùy chọn RA đã bị hạn chế với những tùy chọn được coi là cần thiết cho chức năng mạng cơ bản và cho tất cả các nút được cấu hình với thông tin giống nhau chính xác. Các ví dụ bao gồm các tùy chọn thông tin tiền tố, tùy chọn MTU, v.v… Mặt khác, DHCP thường được ưu tiên để cấu hình các tham số chung hơn và cho các tham số có thể dành riêng cho máy khách. Tuy nhiên, nói chung, có mong muốn chỉ xác định một cơ chế để cấu hình một tùy chọn nhất định, thay vì xác định nhiều cách (khác nhau) của cấu hình thông tin như nhau.

Một vấn đề với việc có nhiều cách để cấu hình thông tin như nhau đó là khả năng tương tác bị ảnh hưởng nếu một máy chủ lựa chọn một cơ chế nhưng nhà khai thác mạng lại chọn một cơ chế khác. Đối với môi trường "đóng", trong đó nhà khai thác mạng có ảnh hưởng đáng kể đến thiết bị nào kết nối với mạng và do đó cơ chế cấu hình nào chúng hỗ trợ, nhà khai thác có thể đảm bảo rằng một cơ chế cụ thể được hỗ trợ bởi tất cả các máy chủ được kết nối. Tuy nhiên, trong các môi trường mở hơn, nơi các thiết bị tùy chọn có thể kết nối (ví dụ: điểm phát sóng Wi-Fi), có thể phát sinh các vấn đề. Để tối đa hóa khả năng tương tác trong môi trường như vậy, máy chủ sẽ cần triển khai nhiều cơ chế cấu hình để đảm bảo khả năng tương tác.

# Các giao thức phát hiện dịch vụ

DNS truyền phát đa hướng (mDNS) và phát hiện dịch vụ dựa trên DNS (DNS-SD) được mô tả tương ứng trong [RFC6762] và [RFC6763]. Các giao thức này, thường được gọi chung là giao thức 'Lời chào' sau khi Apple đặt tên cho chúng, cung cấp phương tiện cho các thiết bị để phát hiện các dịch vụ trong một liên kết cục bộ, và trong trường hợp không có dịch vụ DNS truyền phát đơn hướng, để trao đổi tên thông tin.

Trường hợp các thiết bị sẽ được triển khai trong các mạng mà việc phát hiện dịch vụ sẽ có lợi, mDNS và DNS-SD NÊN được hỗ trợ, ví dụ: đối với những người dùng tìm cách phát hiện máy in hoặc thiết bị hiển thị.

# Hỗ trợ và chuyển đổi IPv4

Các nút IPv6 CÓ THỂ hỗ trợ IPv4.

**Cơ chế chuyển đổi**

**Cơ chế chuyển đổi cơ bản cho các máy chủ và bộ định tuyến IPv6 - RFC 4213**

Nếu một nút IPv6 triển khai cả hai ngăn xếp và đường hầm, thì [RFC4213] PHẢI được hỗ trợ.

# Hỗ trợ ứng dụng

## Thể hiện dạng văn bản địa chỉ IPv6 - RFC 5952

Phần mềm cho phép những người dùng và nhà vận hành nhập vào địa chỉ IPv6 ở dạng văn bản NÊN hỗ trợ "Khuyến nghị cho thể hiện dạng văn bản địa chỉ IPv6" [RFC5952].

## Các giao diện lập trình ứng dụng (API)

Có một số các API liên quan đến IPv6. Tiêu chuẩn này không bắt buộc sử dụng bất kỳ API nào, bởi vì lựa chọn API không liên quan trực tiếp đến hành vi trực tuyến của các giao thức. Tuy nhiên, những nhà triển khai được khuyên nên xem xét cung cấp một API chung hoặc xem xét các API hiện có cho loại chức năng mà họ cung cấp cho các ứng dụng.

- "Các mở rộng giao diện ổ cắm cơ bản cho IPv6" [RFC3493] cung cấp chức năng IPv6 được sử dụng bởi các ứng dụng điển hình. Người triển khai cần lưu ý rằng RFC 3493 đã được quyền lựa chọn và chuẩn hóa hơn nữa bởi giao diện hệ điều hành di động (POSIX) [POSIX].

- "Giao diện chương trình ứng dụng (API) ổ cắm nâng cao cho IPv6" [RFC3542] cung cấp quyền truy cập vào các tính năng IPv6 nâng cao cần thiết cho chẩn đoán và các ứng dụng chuyên biệt khác.

- "API ổ cắm IPv6 để lựa chọn địa chỉ nguồn" [RFC5014] cung cấp các phương tiện ở đó cho phép một ứng dụng khống chế các quy tắc lựa chọn địa chỉ nguồn mặc định của [RFC6724].

- "Các mở rộng giao diện ổ cắm cho bộ lọc nguồn truyền phát đa hướng" [RFC3678] cung cấp hỗ trợ để thể hiện bộ lọc nguồn trên tư cách thành viên nhóm đa hướng.

- "Mở rộng với các ổ cắm API cho IPv6 di động" [RFC4584] cung cấp hỗ trợ ứng dụng để truy cập và bật các tính năng IPv6 di động [RFC6275].

# Tính di động

IPv6 di động [RFC6275] và các thông số kỹ thuật liên quan [RFC3776] [RFC4877] cho phép một nút thay đổi điểm đính kèm của nó trong Internet, đồng thời duy trì (và sử dụng) một địa chỉ cố định. Tất cả giao tiếp sử dụng địa chỉ thường trú tiếp tục diễn ra như mong đợi ngay cả khi nút di chuyển vòng quanh. Xác định IP di động bao gồm các yêu cầu đối với các loại nút như sau:

- Các nút di động.

- Các nút tương ứng có hỗ trợ tối ưu hóa tuyến đường.

- Các máy khách thường trú.

- Tất cả các bộ định tuyến IPv6.

Tại thời điểm hiện tại, IP di động chỉ được triển khai hạn chế và không có triển khai đáng kể, một phần vì ban đầu nó được giả định là môi trường chỉ có IPv6 chứ không phải là Internet hỗn hợp IPv4/IPv6. Hoạt động bổ sung đã được thực hiện để hỗ trợ tính di động trong các mạng IPv4 và IPv6 ở chế độ hỗn hợp [RFC5555].

Cần có thêm kinh nghiệm sử dụng và triển khai với tính di động trước khi có thể khuyến nghị bất kỳ phương pháp tiếp cận cụ thể nào để triển khai rộng rãi trên tất cả các máy chủ và bộ định tuyến. Do đó, Hỗ trợ tính di động trong IPv6 [RFC6275], Hỗ trợ IPv6 di động cho Máy chủ và bộ định tuyến ngăn xếp kép [RFC5555], và các tiêu chuẩn liên quan (chẳng hạn như IPv6 di động với IKEv2 và IPsec [RFC4877]) được coi là CÓ THỂ tại thời điểm này.

IPv6 cho 3GPP [RFC7066] liệt kê ảnh chụp nhanh các chức năng IPv6 được yêu cầu tại thời điểm tiêu chuẩn được xuất bản sẽ cần được triển khai, vượt ra ngoài các khuyến nghị trong tiêu chuẩn này. Ngoài ra, một máy chủ IPv6 3GPP CÓ THỂ triển khai [RFC7278] để phân phối tiền tố IPv6 trên liên kết LAN.

# Bảo mật

Phần này mô tả thông số kỹ thuật bảo mật cho các nút IPv6.

Để đạt được bảo mật trong thực tế là một công việc phức tạp. Các quy trình hoạt động, các giao thức, các cơ chế phân phối khóa, cách tiếp cận quản lý chứng chỉ, v.v…, là tất cả các thành phần tác động đến cấp độ bảo mật thực sự đạt được trong thực tế. Quan trọng hơn, sự thiếu sót hoặc không phù hợp trong bất kỳ thành phần riêng lẻ nào có thể làm giảm đáng kể hiệu quả tổng thể của một phương pháp bảo mật cụ thể.

IPsec có thể cung cấp hoặc là bảo mật đầu cuối giữa các nút hoặc là bảo mật kênh (ví dụ: qua VPN IPsec điểm tới điểm), giúp nó có thể cung cấp truyền thông bảo mật cho tất cả (hoặc một tập hợp con) luồng truyền thông tại lớp IP giữa các cặp nút Internet. IPsec có hai chế độ hoạt động tiêu chuẩn: Chế độ đường hầm và chế độ truyền tải. Trong chế độ đường hầm, IPsec cung cấp bảo mật lớp mạng và bảo vệ toàn bộ gói IP bằng cách đóng gói gói IP gốc và sau đó thêm tiêu đề IP mới. Trong chế độ truyền tải, IPsec cung cấp bảo mật cho lớp truyền tải (ở trên) bằng cách chỉ đóng gói phần lớp truyền tải (ở trên) của gói IP (tức là không thêm tiêu đề IP thứ hai).

Mặc dù IPsec có thể được sử dụng với khóa thủ công trong một số trường hợp, nhưng việc sử dụng như vậy có khả năng ứng dụng hạn chế và không được khuyến khích.

Ngày nay, một loạt các công nghệ và phương pháp tiếp cận bảo mật ngày càng phát triển (ví dụ: IPsec, Bảo mật lớp truyền tải (TLS), bảo mật SHell (SSH), TLS VPNS, v.v…). Không có cách tiếp cận duy nhất nào nổi lên như một công nghệ lý tưởng cho mọi nhu cầu và môi trường. Hơn nữa, IPsec không được xem là công nghệ bảo mật lý tưởng trong mọi trường hợp và không có khả năng thay thế các công nghệ khác.

Trước đây, IPv6 bắt buộc triển khai IPsec và khuyến nghị phương pháp quản lý khóa của IKE. RFC 6434 đã cập nhật khuyến nghị đó bằng cách hỗ trợ kiến ​​trúc IPsec [RFC4301] NÊN cho tất cả các nút IPv6 và tiêu chuẩn này vẫn giữ nguyên đề xuất đó. Lưu ý rằng Kiến trúc IPsec yêu cầu triển khai cả quản lý khóa thủ công và tự động (ví dụ: Phần 4.5 của RFC 4301). Hiện tại, giao thức quản lý khóa tự động được khuyến nghị để triển khai là IKEv2 [RFC7296].

Tiêu chuẩn này thừa nhận rằng tồn tại một loạt các loại thiết bị và môi trường mà các phương pháp tiếp cận bảo mật khác với IPsec có thể được căn chỉnh. Ví dụ, các thiết bị dành cho mục đích đặc biệt có thể chỉ hỗ trợ một số lượng hoặc loại ứng dụng rất hạn chế và cách tiếp cận bảo mật dành riêng cho ứng dụng có thể đủ cho quản lý hoặc cấu hình hạn chế. Ngoài ra, một số thiết bị có thể chạy trên phần cứng cực kỳ hạn chế (ví dụ: cảm biến) trong đó Kiến trúc IPsec đầy đủ không được căn chỉnh.

Bởi vì hầu hết các nền tảng phổ biến hiện nay đều hỗ trợ IPv6 và được phép mặc định, bảo mật IPv6 là một vấn đề đối với các mạng chỉ là IPv4; xem [RFC7123] để hướng dẫn về lĩnh vực này.

## Các yêu cầu

"Kiến trúc bảo mật cho giao thức Internet" [RFC4301] NÊN được hỗ trợ bởi tất cả các nút IPv6. Lưu ý rằng kiến trúc IPsec yêu cầu triển khai cả quản lý khóa thủ công và tự động (ví dụ: Phần 4.5 của [RFC4301]). Hiện tại, giao thức quản lý khóa tự động mặc định để triển khai là IKEv2. Theo yêu cầu trong [RFC4301], các nút IPv6 triển khai Kiến trúc IPsec PHẢI triển khai ESP [RFC4303] và CÓ THỂ triển khai AH [RFC4302].

## Chuyển đổi và thuật toán

Tập hợp các thuật toán bắt buộc phải triển khai hiện tại cho Kiến trúc IPsec được định nghĩa trong yêu cầu triển khai thuật toán mật mã cho ESP và AH [RFC8221]. Các nút IPv6 triển khai kiến trúc IPsec PHẢI tuân thủ các yêu cầu trong [RFC8221]. Các thuật toán mật mã được ưu tiên thường thay đổi thường xuyên hơn các giao thức bảo mật. Do đó, việc triển khai PHẢI cho phép chuyển sang các thuật toán mới, vì RFC 8221 sẽ được thay thế hoặc cập nhật trong tương lai.

Tập hợp các thuật toán bắt buộc phải triển khai hiện tại cho IKEv2 được định nghĩa trong yêu cầu triển khai thuật toán mật mã cho ESP và AH [RFC8247]. Các nút IPv6 triển khai IKEv2 PHẢI tuân thủ các yêu cầu trong [RFC8247] và/hoặc bất kỳ bản cập nhật hoặc thay thế nào trong tương lai cho [RFC8247].

# Chức năng định tuyến cụ thể

Phần này xác định các cân nhắc máy chủ chung cho các nút IPv6 hoạt động như những bộ định tuyến. Hiện tại, phần này không thảo luận chi tiết các yêu cầu định tuyến cụ thể. Đối với trường hợp của bộ định tuyến tại nhà điển hình, [RFC7084] xác định các yêu cầu cơ bản đối với bộ định tuyến biên của khách hàng.

## Tùy chọn cảnh báo định tuyến IPv6 - RFC 2711

Tùy chọn cảnh báo định tuyến IPv6 [RFC2711] là tiêu đề từng chặng IPv6 tùy chọn ở đó được sử dụng cùng với một số giao thức (ví dụ: RSVP [RFC2205] hoặc phát hiện lắng nghe truyền phát đa hướng (MLDv2) [RFC3810]). Tùy chọn cảnh báo định tuyến sẽ cần được triển khai bất cứ khi nào các giao thức bắt buộc phải sử dụng nó. Xem Phần 7.11.

## Phát hiện lân cận cho IPv6 - RFC 4861

Việc gửi quảng cáo định tuyến và xử lý yêu cầu định tuyến PHẢI được hỗ trợ.

Phần 7 của [RFC6275] bao gồm một số phần mở rộng di động cụ thể để phát hiện lân cận. Các bộ định tuyến NÊN triển khai Phần 7.3 và 7.5, ngay cả khi chúng không triển khai chức năng tác nhân tại nhà.

## Tự động định cấu hình địa chỉ trạng thái (DHCPv6) - RFC 3315

Một máy chủ DHCP đơn lẻ ([RFC3315] hoặc [RFC4862]) có thể cung cấp thông tin cấu hình cho các thiết bị được gắn trực tiếp vào một liên kết đã chia sẻ, cũng như cho các thiết bị nằm ở nơi khác trong một vị trí. Truyền thông giữa máy khách và máy chủ DHCP nằm trên các liên kết khác nhau yêu cầu sử dụng các tác nhân chuyển tiếp DHCP trên bộ định tuyến.

Trong các triển khai đơn lẻ, bao gồm một bộ định tuyến và một mạng LAN đơn lẻ hoặc nhiều mạng LAN được gắn với một bộ định tuyến duy nhất, cùng với kết nối WAN, một máy chủ DHCP được nhúng trong bộ định tuyến là một trong những kịch bản triển khai phổ biến (ví dụ: [RFC7084]). Không cần các tác nhân chuyển tiếp trong các kịch bản như vậy.

Trong các kịch bản triển khai phức tạp hơn, chẳng hạn như trong các mạng doanh nghiệp hoặc mạng nhà cung cấp dịch vụ, việc sử dụng DHCP yêu cầu một số mức cấu hình, để định cấu hình tác nhân chuyển tiếp, các máy chủ DHCP, v.v… Trong những môi trường như vậy, máy chủ DHCP thậm chí có thể được chạy trên một máy chủ truyền thống, thay vì là một phần của bộ định tuyến.

Do có nhiều kịch bản triển khai, hỗ trợ cho chức năng máy chủ DHCP trên bộ định tuyến là tùy chọn. Tuy nhiên, các bộ định tuyến được nhắm mục tiêu để triển khai trong các kịch bản phức tạp hơn (như mô tả ở trên) NÊN hỗ trợ chức năng tác nhân chuyển tiếp. Lưu ý rằng "Yêu cầu cơ bản đối với bộ định tuyến biên khách hàng IPv6" [RFC7084] yêu cầu triển khai chức năng máy chủ DHCPv6 trong bộ định tuyến biên khách hàng (CE) IPv6.

## Khuyến nghị độ dài tiền tố IPv6 cho chuyển tiếp hướng thuận - BCP 198

Các nút chuyển tiếp hướng thuận PHẢI tuân theo BCP 198 [RFC7608]; do đó, các nút triển khai IPv6 có thể chuyển tiếp các gói tin PHẢI tuân theo các quy tắc được chỉ định trong Phần 5.1 của [RFC4632].

# Thiết bị bị ràng buộc

Trọng tâm của tiêu chuẩn này là các nút IPv6 chung. Trong phần này, chúng tôi thảo luận ngắn gọn về các cân nhắc đối với các thiết bị bị hạn chế.

Trong trường hợp các nút bị hạn chế, với CPU, bộ nhớ, băng thông hoặc nguồn bị hạn chế, việc hỗ trợ chức năng IPv6 nhất định có thể cần được xem xét do những hạn chế đó. Mặc dù các yêu cầu của tiêu chuẩn này được KHUYẾN CÁO cho tất cả các nút, bao gồm cả các nút bị ràng buộc, các thỏa hiệp có thể cần phải thực hiện trong một số trường hợp nhất định. Khi thực hiện các thỏa hiệp như vậy, khả năng tương tác của các thiết bị cần được xem xét kỹ lưỡng, đặc biệt khi điều này có thể ảnh hưởng đến các nút khác trên cùng một liên kết, ví dụ: chỉ hỗ trợ MLDv1 sẽ ảnh hưởng đến các nút khác.

IETF 6LowPAN (IPv6 qua mạng khu vực cá nhân không dây công suất thấp) WG tạo ra sáu RFC, bao gồm tổng quan chung và tuyên bố vấn đề [RFC4919] (nghĩa là các gói IPv6 được truyền qua mạng IEEE 802.15.4 [RFC4944] và tối ưu hóa ND cho phương tiện đó [RFC6775]).

Các nút IPv6 được cấp nguồn bằng pin NÊN triển khai các khuyến nghị trong [RFC7772].

# Quản lý nút IPv6

Quản lý mạng CÓ THỂ được hỗ trợ bởi các nút IPv6. Tuy nhiên, đối với các nút IPv6 là thiết bị nhúng, quản lý mạng có thể là cách duy nhất để có thể kiểm soát các nút này.

Các giao thức quản lý mạng hiện có bao gồm SNMP [RFC3411], NETCONF [RFC6241] và RESTCONF [RFC8040].

## Các mô đun cơ sở thông tin quản lý (MIB)

Trạng thái bị che khuất của các mô-đun MIB IPv6 cụ thể khác nhau được làm rõ trong [RFC8096].

Sau đây hai mô-đun MIB NÊN được hỗ trợ bởi các nút có hỗ trợ tác nhân SNMP.

### Bảng MIB chuyển tiếp IP

Bảng MIB chuyển tiếp IP [RFC4292] NÊN được hỗ trợ bởi các nút có hỗ trợ tác nhân SNMP.

### Cơ sở thông tin quản lý cho giao thức Internet (IP)

MIB IP [RFC4293] NÊN được hỗ trợ bởi các nút có hỗ trợ tác nhân SNMP.

### Giao diện MIB

Giao diện MIB [RFC2863] NÊN được hỗ trợ bởi các nút có hỗ trợ tác nhân SNMP.

## Các mô hình dữ liệu YANG

Các mô hình dữ liệu YANG sau NÊN được hỗ trợ bởi các nút có hỗ trợ tác nhân NETCONF hoặc RESTCONF.

### Mô hình YANG quản lý IP

Mô hình YANG quản lý IP [RFC8344] NÊN được hỗ trợ bởi các nút có hỗ trợ NETCONF hoặc RESTCONF.

### Mô hình YANG quản lý giao diện

Mô hình YANG quản lý giao diện [RFC8343] NÊN được hỗ trợ bởi các nút có hỗ trợ NETCONF hoặc RESTCONF.

# Các cân nhắc bảo mật

Tiêu chuẩn này không ảnh hưởng trực tiếp đến bảo mật của Internet, ngoài những cân nhắc bảo mật liên quan đến các giao thức riêng lẻ.

Bảo mật cũng đã được thảo luận trong Phần 15 ở trên.

# Các cân nhắc IANA

Tiêu chuẩn này không có hành động IANA.

###### (Tham khảo) CÁC THAY ĐỔI TỪ RFC 6434

Đã có những làm rõ biên tập cũng như bổ sung và cập nhật đáng kể. Mặc dù phần này nêu bật một số những thay đổi, nhưng người đọc không nên dựa vào phần này để có danh sách toàn diện về tất cả các thay đổi.

1. Các phần được tái cấu trúc.

2. Đã thêm 6LoWPAN để liên kết các lớp vì nó có một số triển khai.

3. Đã xóa hồ sơ IPv6 luồng hướng xuống theo yêu cầu (DoD) vì nó chưa được cập nhật.

4. Hỗ trợ MLDv2 được cập nhật thành PHẢI vì các nút bị hạn chế nếu MLDv1 được sử dụng.

5. Tùy chọn RA DNS được yêu cầu vì các thiết bị chỉ SLAAC có thể nhận được DNS; RFC 8106 là PHẢI.

6. Tùy chọn DNS RFC 3646 được yêu cầu để triển khai DHCPv6.

7. Đã thêm RESTCONF và NETCONF như các tùy chọn có thể để quản lý mạng.

8. Đã thêm một phần trên các thiết bị hạn chế.

9. Đã thêm văn bản trên RFC 7934 để giải quyết tính khả dụng của các máy chủ (NÊN).

10. Đã thêm văn bản trên RFC 7844 cho các hồ sơ ẩn danh cho các máy khách DHCPv6.

11. Đã thêm mDNS và DNS-SD dưới dạng phát hiện dịch vụ được cập nhật.

12. Đã thêm RFC 8028 như là một phương pháp NÊN để giải quyết một mạng nhiều tiền tố.

13. Đã thêm ECN RFC 3168 như là NÊN.

14. Đã thêm tham chiếu đến RFC 7123 để bảo mật trên mạng chỉ IPv4.

15. Đã xóa Jumbograms (RFC 2675) vì chúng không được triển khai.

16. Đã cập nhật các RFC bị lỗi lên phiên bản mới của RFC, bao gồm các RFC 2460, 1981, 7321 và 4307.

17. Đã thêm RFC 7772 để xem xét tiêu thụ điện năng.

18. Đã thêm tại sao/64 đường biên để biết chi tiết hơn - RFC 7421.

19. Đã thêm tiền tố IPv6 duy nhất trên mỗi máy chủ để hỗ trợ các mạng IPv6 hiện đang được triển khai.

20. RFC 7066 được làm rõ dưới dạng một kết xuất nhanh cho 3GPP.

21. Đã cập nhật RFC 4191 dưới dạng PHẢI và các máy chủ Loại C là NÊN vì chúng giúp giải quyết các vấn đề về nhiều tiền tố.

22. Đã xóa IPv6 trên ATM vì không có nhiều triển khai.

23. Đã thêm ghi chú trong Phần 6.6 cho Quy tắc 5.5 từ RFC 6724.

24. Đã thêm PHẢI cho BCP 198 để chuyển tiếp các gói IPv6.

25. Đã thêm một tham chiếu đến RFC 8064 để tạo địa chỉ ổn định.

26. Đã thêm văn bản về bảo vệ khỏi các tùy chọn tiêu đề mở rộng quá mức.

27. Đã thêm văn bản về sự nguy hiểm của 1280 MTU UDP, đặc biệt liên quan đến lưu lượng DNS.

28. Đã thêm văn bản để làm rõ hành vi RFC 8200 cho các tiêu đề tiện ích mở rộng không được công nhận hoặc ULP không được công nhận.

29. Đã xóa các địa chỉ email ghi ngày tháng khỏi xác nhận của nhóm thiết kế cho [RFC4294].

###### (Tham khảo) CÁC THAY ĐỔI TỪ RFC 4294 tới RFC 6434

Đã có những làm rõ biên tập cũng như bổ sung và cập nhật đáng kể. Mặc dù phần này nêu bật một số những thay đổi, nhưng người đọc không nên dựa vào phần này để có danh sách toàn diện về tất cả các thay đổi.

1. Đã cập nhật phần giới thiệu để chỉ ra rằng tiêu chuẩn này là một tuyên bố về khả năng ứng dụng và hướng đến các nút chung.

2. Cập nhật đáng kể phần về giao thức di động; đã thêm các tham chiếu và hạ cấp các NÊN trước đó thành CÓ THỂ.

3. Thay đổi phần lớp IP phụ để chỉ liệt kê các RFC có liên quan và thêm một số RFC khác.

4. Đã thêm một phần trên SEND (đó là CÓ THỂ).

5. Đã sửa đổi phần mở rộng quyền riêng tư [RFC4941] để thêm nhiều sắc thái hơn cho khuyến nghị.

6. Đã sửa đổi hoàn toàn phần IPsec/IKEv2, hạ cấp khuyến nghị tổng thể thành NÊN.

7. Khuyến nghị đã nâng cấp DHCPv6 thành NÊN.

8. Đã thêm phần nền về tùy chọn DHCP so với RA, thêm khuyến nghị NÊN cho cấu hình DNS qua RA (RFC 6106) và xóa các khuyến nghị DHCP.

9. Đã thêm khuyến nghị rằng các bộ định tuyến thực hiện Mục 7.3 và 7.5 của [RFC6275].

10. Đã thêm một con trỏ vào tài liệu làm rõ mạng con [RFC5942].

11. Đã thêm văn bản "Chia sẻ tải từ máy chủ tới bộ định tuyến IPv6" [RFC4311] NÊN được triển khai.

12. Đã thêm tham chiếu đến [RFC5722] (các phân đoạn chồng chéo) và làm cho nó PHẢI triển khai.

13. NÊN đưa ra "Khuyến nghị cho biểu diễn văn bản địa chỉ IPv6" [RFC5952].

14. Đã xóa đề cập đến tên ủy quyền (DNAME) khỏi cuộc thảo luận về [RFC3363].

15. Nhiều bản cập nhật để phản ánh các phiên bản mới hơn của tài liệu IPv6, bao gồm [RFC3596], [RFC4213], [RFC4291] và [RFC4443].

16. Đã xóa thảo luận về các cờ "Được quản lý" và "Khác" trong RA. Hiện tại không có sự đồng thuận về cách xử lý các cờ này, và thảo luận về ngữ nghĩa của chúng đã bị xóa trong bản cập nhật gần đây nhất của tự động cấu hình địa chỉ phi trạng thái [RFC4862].

17. Đã thêm nhiều tài liệu tham chiếu khác vào tài liệu IPv6 tùy chọn.

18. NÊN đưa ra "Khuyến nghị cho biểu diễn văn bản địa chỉ IPv6" [RFC5952].

19. Đã cập nhật phần MLD để bao gồm tham chiếu đến MLD tải trọng nhẹ [RFC5790].

20. Đã thêm khuyến nghị NÊN cho "Tham chiếu định tuyến mặc định và các định tuyến cụ thể hơn" [RFC4191].

21. Tạo NÊN cho "Thông số kỹ thuật nhãn luồng IPv6" [RFC6437].

**THƯ MỤC TÀI LIỆU THAM KHẢO**

QCVN 89:2015/BTTTT Quy chuẩn kỹ thuật quốc gia về IPv6 đối với thiết bị nút.

RFC 8504 (2019) “IPv6 Node Requirements”.

[RFC793] Postel, J., "Transmission Control Protocol", STD 7, RFC 793, DOI 10.17487/RFC0793, September 1981.

[RFC2205] Braden, R., Ed., Zhang, L., Berson, S., Herzog, S., and S. Jamin, "Resource ReSerVation Protocol (RSVP) -- Version 1 Functional Specification", RFC 2205, DOI 10.17487/RFC2205, September 1997).

[RFC2464] Crawford, M., "Transmission of IPv6 Packets over Ethernet Networks", RFC 2464, DOI 10.17487/RFC2464, December 1998).

[RFC2491] Armitage, G., Schulter, P., Jork, M., and G. Harter, "IPv6 over Non-Broadcast Multiple Access (NBMA) networks", RFC 2491, DOI 10.17487/RFC2491, January 1999.

[RFC2590] Conta, A., Malis, A., and M. Mueller, "Transmission of IPv6 Packets over Frame Relay Networks Specification", RFC 2590, DOI 10.17487/RFC2590, May 1999.

[RFC2874] Crawford, M. and C. Huitema, "DNS Extensions to Support IPv6 Address Aggregation and Renumbering", RFC 2874, DOI 10.17487/RFC2874, July 2000.

[RFC2923] Lahey, K., "TCP Problems with Path MTU Discovery", RFC 2923, DOI 10.17487/RFC2923, September 2000.

[RFC3146] Fujisawa, K. and A. Onoe, "Transmission of IPv6 Packets over IEEE 1394 Networks", RFC 3146, DOI 10.17487/RFC3146, October 2001.

[RFC3363] Bush, R., Durand, A., Fink, B., Gudmundsson, O., and T. Hain, "Representing Internet Protocol version 6 (IPv6) Addresses in the Domain Name System (DNS)", RFC 3363, DOI 10.17487/RFC3363, August 2002.

[RFC3493] Gilligan, R., Thomson, S., Bound, J., McCann, J., and W. Stevens, "Basic Socket Interface Extensions for IPv6", RFC 3493, DOI 10.17487/RFC3493, February 2003.

[RFC3542] Stevens, W., Thomas, M., Nordmark, E., and T. Jinmei, "Advanced Sockets Application Program Interface (API) for IPv6", RFC 3542, DOI 10.17487/RFC3542, May 2003.

[RFC3646] Droms, R., Ed., "DNS Configuration options for Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3646, DOI 10.17487/RFC3646, December 2003.

[RFC3678] Thaler, D., Fenner, B., and B. Quinn, "Socket Interface Extensions for Multicast Source Filters", RFC 3678, DOI 10.17487/RFC3678, January 2004.

[RFC3776] Arkko, J., Devarapalli, V., and F. Dupont, "Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents", RFC 3776, DOI 10.17487/RFC3776, June 2004.

[RFC3971] Arkko, J., Ed., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, DOI 10.17487/RFC3971, March 2005.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, DOI 10.17487/RFC3972, March 2005.

[RFC4191] Draves, R. and D. Thaler, "Default Router Preferences and More-Specific Routes", RFC 4191, DOI 10.17487/RFC4191, November 2005.

[RFC4294] Loughney, J., Ed., "IPv6 Node Requirements", RFC 4294, DOI 10.17487/RFC4294, April 2006.

[RFC4302] Kent, S., "IP Authentication Header", RFC 4302, DOI 10.17487/RFC4302, December 2005.

[RFC4338] DeSanti, C., Carlson, C., and R. Nixon, "Transmission of IPv6, IPv4, and Address Resolution Protocol (ARP) Packets over Fibre Channel", RFC 4338, DOI 10.17487/RFC4338, January 2006.

[RFC4380] Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, DOI 10.17487/RFC4380, February 2006.

[RFC4429] Moore, N., "Optimistic Duplicate Address Detection (DAD) for IPv6", RFC 4429, DOI 10.17487/RFC4429, April 2006.

[RFC4584] Chakrabarti, S. and E. Nordmark, "Extension to Sockets API for Mobile IPv6", RFC 4584, DOI 10.17487/RFC4584, July 2006.

[RFC4821] Mathis, M. and J. Heffner, "Packetization Layer Path MTU Discovery", RFC 4821, DOI 10.17487/RFC4821, March 2007.

[RFC4877] Devarapalli, V. and F. Dupont, "Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture", RFC 4877, DOI 10.17487/RFC4877, April 2007.

[RFC4884] Bonica, R., Gan, D., Tappan, D., and C. Pignataro, "Extended ICMP to Support Multi-Part Messages", RFC 4884, DOI 10.17487/RFC4884, April 2007.

[RFC4890] Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, DOI 10.17487/RFC4890, May 2007.

[RFC4919] Kushalnagar, N., Montenegro, G., and C. Schumacher, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals", RFC 4919, DOI 10.17487/RFC4919, August 2007.

[RFC4944] Montenegro, G., Kushalnagar, N., Hui, J., and D. Culler, "Transmission of IPv6 Packets over IEEE 802.15.4 Networks", RFC 4944, DOI 10.17487/RFC4944, September 2007.

[RFC5014] Nordmark, E., Chakrabarti, S., and J. Laganier, "IPv6 Socket API for Source Address Selection", RFC 5014, DOI 10.17487/RFC5014, September 2007.

[RFC5072] Varada, S., Ed., Haskins, D., and E. Allen, "IP Version 6 over PPP", RFC 5072, DOI 10.17487/RFC5072, September 2007.

[RFC5121] Patil, B., Xia, F., Sarikaya, B., Choi, JH., and S. Madanapalli, "Transmission of IPv6 via the IPv6 Convergence Sublayer over IEEE 802.16 Networks", RFC 5121, DOI 10.17487/RFC5121, February 2008.

[RFC5555] Soliman, H., Ed., "Mobile IPv6 Support for Dual Stack Hosts and Routers", RFC 5555, DOI 10.17487/RFC5555, June 2009.

[RFC6275] Perkins, C., Ed., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, DOI 10.17487/RFC6275, July 2011.

[RFC6563] Jiang, S., Conrad, D., and B. Carpenter, "Moving A6 to Historic Status", RFC 6563, DOI 10.17487/RFC6563, March 2012.

[RFC6980] Gont, F., "Security Implications of IPv6 Fragmentation with IPv6 Neighbor Discovery", RFC 6980, DOI 10.17487/RFC6980, August 2013.

[RFC7066] Korhonen, J., Ed., Arkko, J., Ed., Savolainen, T., and S. Krishnan, "IPv6 for Third Generation Partnership Project (3GPP) Cellular Hosts", RFC 7066, DOI 10.17487/RFC7066, November 2013.

[RFC7084] Singh, H., Beebee, W., Donley, C., and B. Stark, "Basic Requirements for IPv6 Customer Edge Routers", RFC 7084, DOI 10.17487/RFC7084, November 2013.

[RFC7123] Gont, F. and W. Liu, "Security Implications of IPv6 on IPv4 Networks", RFC 7123, DOI 10.17487/RFC7123, February 2014.

[RFC7278] Byrne, C., Drown, D., and A. Vizdal, "Extending an IPv6 /64 Prefix from a Third Generation Partnership Project (3GPP) Mobile Interface to a LAN Link", RFC 7278, DOI 10.17487/RFC7278, June 2014.

[RFC7371] Boucadair, M. and S. Venaas, "Updates to the IPv6 Multicast Addressing Architecture", RFC 7371, DOI 10.17487/RFC7371, September 2014.

[RFC7421] Carpenter, B., Ed., Chown, T., Gont, F., Jiang, S., Petrescu, A., and A. Yourtchenko, "Analysis of the 64-bit Boundary in IPv6 Addressing", RFC 7421, DOI 10.17487/RFC7421, January 2015.

[RFC7721] Cooper, A., Gont, F., and D. Thaler, "Security and Privacy Considerations for IPv6 Address Generation Mechanisms", RFC 7721, DOI 10.17487/RFC7721, March 2016.

[RFC7739] Gont, F., "Security Implications of Predictable Fragment Identification Values", RFC 7739, DOI 10.17487/RFC7739, February 2016.

[RFC7772] Yourtchenko, A. and L. Colitti, "Reducing Energy Consumption of Router Advertisements", BCP 202, RFC 7772, DOI 10.17487/RFC7772, February 2016.

[RFC7844] Huitema, C., Mrugalski, T., and S. Krishnan, "Anonymity Profiles for DHCP Clients", RFC 7844, DOI 10.17487/RFC7844, May 2016.

[RFC7934] Colitti, L., Cerf, V., Cheshire, S., and D. Schinazi, "Host Address Availability Recommendations", BCP 204, RFC 7934, DOI 10.17487/RFC7934, July 2016.

[RFC8087] Fairhurst, G. and M. Welzl, "The Benefits of Using Explicit Congestion Notification (ECN)", RFC 8087, DOI 10.17487/RFC8087, March 2017.

[RFC8096] Fenner, B., "The IPv6-Specific MIB Modules Are Obsolete", RFC 8096, DOI 10.17487/RFC8096, April 2017.

[RFC8273] Brzozowski, J. and G. Van de Velde, "Unique IPv6 Prefix per Host", RFC 8273, DOI 10.17487/RFC8273, December 2017.

[POSIX] IEEE, "Information Technology -- Portable Operating System Interface (POSIX(R)) Base Specifications, Issue 7", IEEE Std 1003.1-2017, DOI: 10.1109/IEEESTD.2018.8277153, January 2018.

[USGv6] National Institute of Standards and Technology, "A Profile for IPv6 in the U.S. Government - Version 1.0", NIST SP500-267, July 2008.