

TCVN

TIÊU CHUẨN QUỐC GIA

TCVN 11237-3:2015

Xuất bản lần 1

**GIAO THỨC CẤU HÌNH ĐỘNG CHO INTERNET PHIÊN BẢN
6 (DHCPV6) - PHẦN 3: CÁC TÙY CHỌN CẤU HÌNH DNS**

*Dynamic host configuration protocol for IPv6 (DHCPv6) - Part 3: DNS configuration options for
dynamic host configuration protocol for IPv6 (DHCPv6)*

HÀ NỘI - 2015

Mục lục

1 Phạm vi áp dụng.....	5
2 Tài liệu viện dẫn.....	5
3 Thuật ngữ và định nghĩa.....	5
4 Tùy chọn máy chủ tên miền DNS đệ quy.....	6
5 Tùy chọn danh sách tìm kiếm miền	6
6 Sự xuất hiện của các tùy chọn.....	7
7 Vấn đề bảo mật	7
8 Vấn đề liên quan đến IA_NA.....	7
Thư mục tài liệu tham khảo.....	8

Lời nói đầu

TCVN 11237-3:2015 được xây dựng trên cơ sở tài liệu IETF RFC 3646:2003 (Các tùy chọn cấu hình DNS cho DHCPv6) của Nhóm đặc trách về kỹ thuật Internet (IETF).

TCVN 11237-3:2015 do Vụ Khoa học và Công nghệ 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.

Bộ tiêu chuẩn TCVN 11237 Giao thức cấu hình động cho Internet phiên bản 6 (DHCPv6) gồm ba phần:

- TCVN 11237-1:2015, Phần 1: Đặc tả giao thức;
- TCVN 11237-2:2015, Phần 2: Dịch vụ DHCP không giữ trạng thái cho IPv6;
- TCVN 11237-3:2015, Phần 3: Các tùy chọn cấu hình DNS.

Giao thức cấu hình động cho Internet phiên bản 6 (DHCPv6) - Phần 3: Các tùy chọn cấu hình DNS cho DHCPv6

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) - Part 3: DNS Configuration options for DHCPv6

1 Phạm vi áp dụng

Tiêu chuẩn này mô tả hai tùy chọn để chuyển thông tin cấu hình liên quan đến dịch vụ tên miền (DNS) trong TCVN 11237-1:2015.

Trong Tiêu chuẩn này DHCP được hiểu là DHCPv6.

2 Tài liệu viện dẫn

Tài liệu viện dẫn sau rất 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).

TCVN 11237-1:2015, Giao thức cấu hình động cho Internet phiên bản 6 (DHCPv6) – Phần 1: Đặc tả giao thức;

IETF RFC 1035, Domain names - implementation and specification, 1987 (*Các tên miền – đặc điểm kỹ thuật và thực hiện*);

IETF RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, 1997 (*Các từ khóa dùng trong RFC để chỉ báo các mức độ yêu cầu*);

IETF RFC 2535, Domain Name System Security Extensions, 1999 (*Các mở rộng bảo mật cho hệ thống tên miền*);

IETF RFC 1536, Common DNS Implementation Errors and Suggested Fixes, 1993 (*Các lỗi thực thi và khuyến nghị sửa lỗi thường gặp cho DNS*).

3 Thuật ngữ và định nghĩa

Tiêu chuẩn này sử dụng các thuật ngữ và định nghĩa được nêu trong TCVN 11237-1:2015 và các thuật ngữ và định nghĩa sau:

3.1

Bộ phân giải DNS (DNS Resolver)

DNS phía máy khách có trách nhiệm khởi tạo và thiết đặt trình tự của các truy vấn để có thể dịch đổi đầy đủ, hoàn thiện của một tìm kiếm đã khởi tạo. Ví dụ, dịch đổi một tên miền thành một địa chỉ IP.

3.2

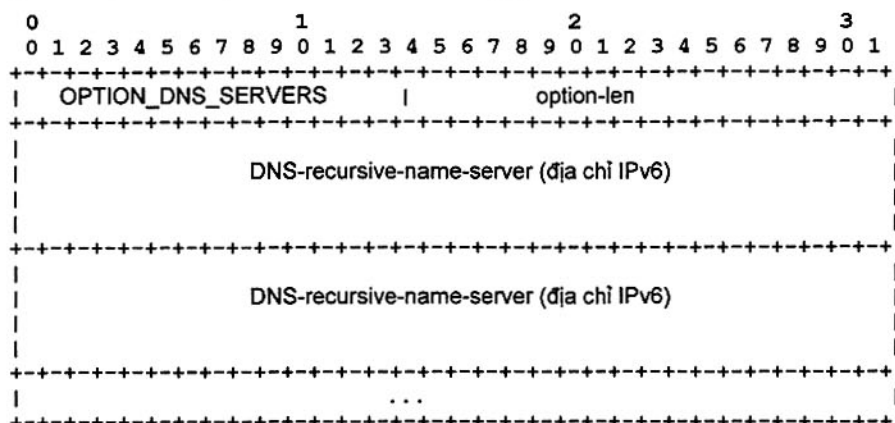
FQDN (Fully Qualified Domain Name)

Địa chỉ tên miền toàn bộ, bao gồm cả tên của máy chủ lưu trữ tên miền và tên miền cấp cao nhất.

4 Tùy chọn máy chủ tên miền DNS đệ quy

Tùy chọn máy chủ tên miền DNS đệ quy cung cấp danh sách một hoặc nhiều địa chỉ IPv6 của các máy chủ tên miền DNS đệ quy mà bộ phân giải DNS của máy khách có thể gửi các truy vấn DNS tới các địa chỉ đó. Các máy chủ DNS được liệt kê theo thứ tự ưu tiên để bộ phân giải DNS của máy khách sử dụng.

Định dạng của Tùy chọn máy chủ tên miền DNS đệ quy như sau:



Mã tùy chọn : OPTION_DNS_SERVERS (mã 23)

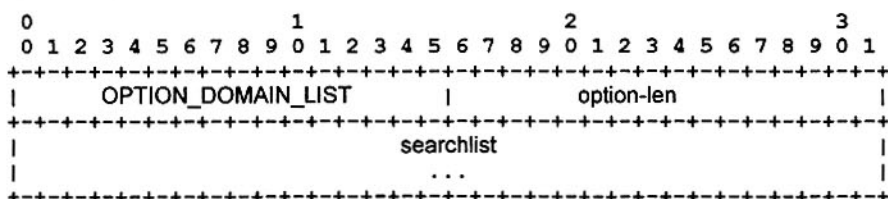
Option-len : Độ dài Danh sách các máy chủ tên miền DNS đệ quy tính bằng octet và phải là bội của 16

DNS-recursive-name-server : Địa chỉ IPv6 của mỗi máy chủ tên miền DNS đệ quy

5 Tùy chọn danh sách tìm kiếm miền

Tùy chọn danh sách tìm kiếm miền xác định danh sách tìm kiếm miền mà máy khách sử dụng khi phân giải tên máy chủ (hostname) với DNS. Tùy chọn này không áp dụng đối với các cơ chế phân giải tên khác.

Định dạng của Tùy chọn danh sách tìm kiếm miền như sau:



Mã tùy chọn: OPTION_DOMAIN_LIST (mã 24)

option-len: Độ dài của trường "searchlist" tính bằng octet

searchlist: Bản danh sách tên miền trong danh sách tìm kiếm miền

Danh sách tên miền trong "searchlist" PHẢI được mã hóa như quy định trong Điều 8 - Biểu diễn và sử dụng các tên miền trong TCVN 11237-1:2015.

6 Sự xuất hiện của các tùy chọn

Tùy chọn máy chủ tên miền DNS đệ quy **KHÔNG ĐƯỢC** xuất hiện trong các bản tin trừ các bản tin sau đây: Solicit, Advertise, Request, Renew, Rebind, Information-Request và Reply.

Tùy chọn danh sách tìm kiếm miền **KHÔNG ĐƯỢC** xuất hiện trong các bản tin trừ các bản tin sau đây: Solicit, Advertise, Request, Renew, Rebind, Information-Request và Reply.

7 Vấn đề bảo mật

Tùy chọn máy chủ tên miền DNS đệ quy có thể được sử dụng bởi một máy chủ DHCP xâm nhập làm cho các máy khách DHCP gửi các yêu cầu DNS đến máy chủ tên miền DNS đệ quy xâm nhập. Kết quả là các yêu cầu DNS sai hướng có thể được sử dụng để giả mạo các tên DNS.

Để tránh các cuộc tấn công bằng Tùy chọn máy chủ tên miền DNS đệ quy, máy khách DHCP **NÊN** yêu cầu xác thực DHCP (xem Điều 21 - Xác thực các bản tin DHCP trong TCVN 11237-1:2015) trước khi cài đặt danh sách các máy chủ tên miền DNS đệ quy có được thông qua DHCP đã xác thực.

Tùy chọn danh sách tìm kiếm miền có thể được sử dụng bởi một máy chủ DHCP thâm nhập làm cho các máy khách DHCP tìm kiếm thông qua các miền không hợp lệ với các tên miền được xác định một cách chưa hoàn chỉnh. Kết quả là các quá trình tìm kiếm sai hướng này có thể được sử dụng để giả mạo máy chủ DNS. Chú ý rằng việc hỗ trợ cho DNSSEC sẽ không ngăn chặn việc tấn công này, bởi vì các bản ghi tài nguyên trong các miền không chính xác có thể được xác định là hợp pháp.

Mức độ mà máy chủ dễ bị tấn công thông qua tùy chọn tìm kiếm miền không chính xác được xác định một phần bởi bộ phân giải DNS. RFC 1535 chứa thông tin về các điểm yếu bảo mật liên quan đến ẩn hoặc hiện các danh sách tìm kiếm miền và cung cấp các khuyến nghị liên quan đến việc xử lý danh sách tìm kiếm của bộ phân giải. Điều 6 của RFC 1536 cũng chỉ ra phần dễ bị tấn công này và khuyến nghị đối với các bộ phân giải:

- Sử dụng các danh sách tìm kiếm chỉ khi đã hiển rõ; không cần sử dụng các danh sách tìm kiếm ẩn.
- Phân giải tên chứa các chấm (.) bất kỳ bằng việc đầu tiên thử tên miền đó như một FQDN và nếu không thành công thì thêm các tên trong danh sách tìm kiếm.
- Phân giải tên không chứa các dấu chấm (.) bằng cách thêm danh sách tên hợp lý, nhưng một lần nữa không cần sử dụng các danh sách tìm kiếm ẩn.

Để giảm thiểu khả năng bị tấn công, khuyến nghị rằng:

- Các máy chủ triển khai tùy chọn tìm kiếm tên cũng **NÊN** triển khai các khuyến nghị danh sách tìm kiếm trong Điều 6 của RFC 1536;
- Nếu các tham số DNS như là danh sách miền hoặc các máy chủ DNS được cấu hình nhân công, thì các tham số này **KHÔNG NÊN** bị kiểm soát bởi DHCP;
- Máy chủ **NÊN** yêu cầu sử dụng xác thực DHCP (xem Điều 21 - Xác thực các bản tin DHCP trong TCVN 11237-1:2015) trước khi chấp nhận tùy chọn tìm kiếm miền.

8 Vấn đề liên quan đến IANA

IANA ấn định một mã tùy chọn cho Tùy chọn máy chủ tên miền DNS đệ quy (mã 23) và Tùy chọn danh sách tìm kiếm miền (mã 24) từ không gian mã tùy chọn DHCP quy định trong Điều 24 - Các vấn đề về IA_NA trong TCVN 11237-1:2015.

Thư mục tài liệu tham khảo

1. IETF RFC 1034, Domain names - concepts and facilities, 1987 (Tên miền – các khái niệm và thiết bị);
 2. IETF RFC 1535, A Security Problem and Proposed Correction With Widely Deployed DNS Software, 1993 (Vấn đề an ninh và hiệu chỉnh được đề xuất đối với phần mềm DNS triển khai diện rộng);
 3. IETF RFC 3397, Dynamic Host Configuration Protocol (DHCP) Domain Search Option, 2002 (Tùy chọn tìm kiếm tên miền của DHCP).
-