Zone Suffix Option for DHCPv6
<Draft-yan-dhc-dhcpv6-opt-dnszone-02.txt>

December 24, 2004

Abstract

This document specifies a new DHCPv6 (DHCP for IPv6) option which is passed from an DHCPv6 server to an DHCPv6 client to specify the zone suffix name used to construct and perform domain name update.

Copyright (C) The Internet Society (2004). All Rights Reserved.
1.0 Introduction

This document describes a new option for DHCPv6 [2] that provides a mechanism for the transfer of a zone suffix name. Using this option, an IPv6 device, which works as a DHCPv6 client, can configure the zone suffix name automatically.

For example, a service provider would use this option to transfer a zone suffix name to a Customer Premise Equipment (CPE) device acting as a router between the subscriber’s internal network and the service provider’s core network.

The configured zone suffix name is intended to be used by the IPv6 device to perform DNS update for the hosts inside its local network. The DNS update can be realized by several methods. The DHCPv6 Client FQDN Option [6] provides a mechanism to exchange client’s FQDN information during a stateful DHCPv6 session. DNS update mechanism for IPv6 stateless configuration can be defined in the future.

1.1 Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [4].

This document should be read in conjunction with the DHCPv6 specification, RFC 3315 [2]. Definitions for terms and acronyms used in this document are defined in RFC 3315 and RFC 3633 [3].

2.0 Zone Suffix Option

The zone suffix option is used to carry a zone suffix to the DHCPv6 client, which will be used to construct and update the domain name for the hosts in local network.

The format of the zone suffix option is:

```
0                   1                   2                   3
      0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|             Type            |            Length               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
|                                                               |
|                   ~                            zone suffix                  |
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
Type:         16-bits identifier of the type of option (TBD).
```
Length:       Length of the "zone suffix" field in octets.

zone suffix:  The specification of a zone suffix.

The zone suffix in the 'zone suffix' MUST include only one item, and
MUST be encoded as specified in section "Representation and use of
domain names" of RFC3315.

2.1 Usage

In stateful DHCPv6, the zone suffix option MUST only appear in
IA_PD-options field of IA_PD option (see [3]) and apply to all
prefixes for that binding. One IA_PD-options field MUST include none
or only one zone suffix option.

In stateless DHCPv6, the zone suffix option can appear in the
client's message options field in the transaction.

Stateful DHCPv6 server may allocate different zone suffix name to
different clients. This can avoid frequent domain name conflicts when
performing DNS update in large network. The mechanism through which
the server selects different zone suffix name for client is not
specified in this document.

3.0 Example and applicability

```
+------+
| Node +--+
+------+
           |
| Node ++++
+------+

: +-------+ +------------------+          +----------+
|   | ISP Core|                        |          |
++-+ CPE  +----|Aggregation device|---|--|          |

: +-------+ +------------------+
|   | Network |
++-+          +----------+
| Node ++++
+------+

Subscriber network                ISP network
```

The above figure shows a typical usage of the zone suffix option.
In this model, ISP has the ISP level domain name suffix (e.g.
example.com).
The CPE in the subscriber network, which acts as a requesting router, initiates a DHCP session with the router in ISP network. An IPv6 prefix, along with the corresponding zone suffix name (i.e. example.com) will be transferred to the CPE.

The zone suffix name can then be used to construct a domain name for the hosts in subscriber network, by an embedded DHCPv6 server in CPE or by other means of DNS update mechanism for stateless IPv6 configuration.

To avoid frequent domain name conflicts, aggregation device might allocate different zone suffix name for the CPE. An example way can be selection based on an external authority such as a RADIUS server, in which an unique zone suffix name prefix, called "home name", are negotiated between user and ISP when subscribing. For example, "user1.example.com" and "user2.example.com".

4.0 Security Considerations

Security considerations in DHCP are described in section 23, "Security Considerations" of RFC 3315.

A rogue DHCP server can issue bogus zone suffix to a client. This may cause wrong domain name update.

A malicious client may be able to mount a denial of service attack by repeated DHCP requests for zone suffix, thus exhausts the DHCP server's resource.

Currently, it is difficult for DHCP servers to develop much confidence in the identities of its clients, given the absence of entity authentication from the DHCP protocol itself. To guard against attack, DHCP Authentication as described in section 21 of RFC 3315 can be used.

Copyright notice

Copyright (C) The Internet Society (2004). This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.
References


Author Information:

Renxiang Yan
Yinglan Jiang
Luoning Gui
Research & Innovation Center
Alcatel Shanghai Bell Co., Ltd.
388#, NingQiao Road, Pudong Jingqiao
Shanghai 201206 P.R. China
Phone: +86 (21) 5854-1240

Email: renxiang.yan@alcatel-sbell.com.cn
Yinglan.jiang@alcatel-sbell.com.cn
Luoning.gui@alcatel-sbell.com.cn