Address Selection Policy Configuration by DHCPv6 Option
draft-sun-mif-address-policy-dhcp6-01.txt

Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html

This Internet-Draft will expire on September 10, 2009.

Copyright Notice

Copyright (c) 2009 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document.

Abstract
For hosts with multiple interfaces, the problem is how to make it run several applications simultaneously on variant interfaces such as GPRS, Wifi etc. To achieve this, one way is to select appropriate IP address so that the packets can be sent to the corresponding interface for forwarding. RFC 3484 defines a “policy table” for default IP address selection. This document extends the DHCPv6 option message so that the policy table can be dynamically updated.

Table of Contents

1. Introduction...................................................2
2. Solutions......................................................4
   2.1. Route Table Updation......................................4
   2.2. The Option of DHCPv6.................................4
   2.3. Some Considerations of the DHCPv6 Option............6
      2.3.1. Conflict of Route Rules..........................6
      2.3.2. Application Situations............................6
      2.3.3. Not Limited to DHCP Servers......................6
3. IANA Considerations...........................................6
4. Conclusions....................................................
5. References..................................................
   5.1. Normative References....................................7
   5.2. Informative References..................................7

1. Introduction

A host such as a laptop or a smart-phone may have multiple interfaces for connections, e.g., a wired Ethernet LAN, a 802.11 LAN, a 3G cell network, one or multiple VPNs or tunnels. In view of more and more versatile applications, users may expect a host to utilize several interfaces at the same time.

If the source IP address is selected and bind by an application, then the application can use certain interface in this way. However, source IP addresses are generally added by sockets in IP layer. According to [RFC 1122], all the packets whose destination IP addresses are not specified in the route table will be send to a default gateway for forwarding. Accordingly, the IP address corresponding to the default gateway is chosen as the source IP address.

To avoid all packets passing through the same interface corresponding to the default gateway, the approach in this document configures the IP address “policy table” defined in [RFC 3484]
To address multi-homed problems in a flexible way, [I-D-hui-mif-dhcpv4-routing-00] extends DHCPv4 through introducing TOS and specific routes into DHCP options. This document considers IPv6 situations. The approach presented in [I-D. sun-mif-route-config-dhcp6-00] is an approach which extends DHCP option for sending route information. The route table and the address selection policy table can be used jointly to let multiple interfaces work simultaneously.

2. Solution of Multiple Interface Usage

The procedures of configuring policy table of address selection are depicted in Figure 1.

The policy table configure procedures are shown as steps a1 to a3.

- a1) An interface sends Information-requirement when the connection is established or when an existing connection receives reconfiguration message from the server.

- a2) The server sends policy rules through DHCPv6 option as to be defined in Section 3.2.

- a3) The policy rules received from the interface is used to configure the policy table of the host.

The procedures that an application employs an interface for network access are depicted in Figure 1 as steps b1 to b4.

- b1) An application calls sockets to build IP packets.

- b2) The socket determines the destination and selects source address based on the policy table.

- b3) The socket sends packets to the corresponding interface.

- b4) The interface will forward the packets to the next hop (the corresponding gateway).
3. DHCPv6 Option Extensions

3.1. Host and Server Behavior

The host must include 'Option Request' option to let the server know the option the host interested. The request option code is set as the 'Address Policy' defined in 3.2.

The server constructs a Reply message to provide IP address policy rules to the host. Also, a server may send a Reconfigure Message to the host. The host may initiate a request when receiving the Reconfigure message for the host.

3.2. Address Policy Option

The DHCPv6 option is extended to contain multiple pieces of default address selection policy rules. Each piece of rules contains address, preference and label which are properties defined in [RFC3484]. The ADDRESS_POLICY option is depicted in Figure 2.
Figure 2 The Address Policy Option.

option-code OPTION_ADDRESS_POLICY (should be defined by IANA).

option-len length of the route rule field in octets.

IF-Based N  A flag used to indicate whether the Nth rule is
''interface Based'' (=1) or ''host based'' (=0).

Address   Prefix Len Length of an IPv6 destination address prefix, an
          8-bit unsigned integer ranging from 0 to 128.

Address Prefix The address prefix

Preference A number identifies the priority of one type of IP address.

Label     A number that used to mark the Nth rule correspondence
          between source and destination address.

The ''IF-Based'' flag is used to indicate whether the rule applies only
to the interface that received the DHCP reply message or the rule is
''host based'' and applies to all the interfaces. This flag is
introduced for merging route policies that received from multiple
interfaces.
3.3. Some Considerations of the DHCPv6 Option

3.3.1. Conflict of A Policy Table

For the situations where the rule in the policy table conflicts with one previous policy table, the latter one will override the previous rule.

3.3.2. Application Situations

There are two situations when DHCPv6 is applied, i.e., with or without stateless autoconfiguration. For the stateless case, since the address has been configured based on the link-local/site-local address, the DHCPv6 is used to obtain options.

3.3.3. Not Limited to DHCP Servers

The solution presented in this document is with the context of DHCP message. It should be pointed out that similar message may not be conveyed by certain node in the network instead of a DHCP server. Router solicitation and advertisement are also potential approach to convey the

4. IANA Considerations

The option code of ADDRESS_POLICY will be defined by IANA.

5. Security Considerations

The security issues in this document are similar with those that have been met when using DHCPv6 options.

The interface selection is affected by the routing and address selection rules sent from servers. Therefore, incorrect information received by hosts will cause improper interface selection leading to bad user experiences. Attacks such as deny of services (DoS) or man-in-the-middle may redirect host’s solicitation, change the information or flood the host with invalidate messages. Approaches to guarantee the communication securities between hosts and servers should be applied based on the network access types of the interfaces.
6. References

6.1. Normative References


6.2. Informative References


[I-D.hui-mif-dhcpv4-routing-00] Hui, M., and Deng, H. "Extension of DHCPv4 for policy routing of multiple interfaces terminal,'', draft-hui-mif-dhcpv4-routing-00(work in progress), February 2009

[I-D.yang-mif-req] Yang, P., Seite, P., Williams, C., and J. Qin, "Requirements on multiple Interface (MIF) of simple IP", draft-yang-mif-req-00 (work in progress), March 2009.

Authors’ Addresses

Tao Sun
China Moible
53A,Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China
Email: suntao@chinamobile.com

Hui Deng
China Moible
53A,Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China
Email: denghui@chinamobile.com

Xiaodong Duan
China Moible
53A,Xibianmennei Ave.,
Xuanwu District,
Beijing 100053
China
Email: duanxiaodong@chinamobile.com