Internet Engineering Task Force
Internet-Draft
Intended status: Standards Track
Expires: April 15, 2013

T. Yang
L. Li
Q. Ma
China Mobile
Oct 12, 2012

Weakening Aggregated Traffic of DHCP Discover Messages
draft-yang-sunset4-weaken-dhcp-00

Abstract

This document proposes two methods to mitigate aggregated traffic caused by discover messages the dual stack host send to the server.

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). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on April 15, 2013.

Copyright Notice

Table of Contents

1. Introduction

In RFC3315 [RFC3315, DHCPv6], SOL_MAX_RT is defined in DHCPv6 to prevent the frequently requesting of clients, which reduce the aggregated traffic. But in RFC2131 [RFC2131, DHCPv4], there are not corresponding IPv4 definitions or options for client's behavior if the server does not respond for the Discover messages.

In some cases, this will lead to an unacceptably high volum of aggregated traffic at a DHCP server, especially in the "Dual-Stack host/network + IPv6-Only DHCP server" scenario:

As everyone knows, our network is changing from IPv4-Only to Dual-Stack, and even IPv6-Only in the near future. We may turn off some IPv4 services gradually, such as DHCP. If a Dual-Stack host initials DHCP Discover messages through the link to a DHCPv6-Only server, it cannot get any response. Then the host will re-broadcast the messages endlessly, that may cause the aggregated traffic.

In this document, we propsed two methods to solve this problem, creating a new option in DHCPv6 or in RS/RA, described as below.

2. Requirements Language

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 [RFC2119].

3. Potential Problems

RFC2131 [RFC2131] defines the interaction between the DHCP server and clients. There are no specific discription for client's operation when the client does not receive the DHCPOFFER in response to its DHCPDISCOVER message. In normal IPv4 environment, clients will flood DHCPDISCOVER messages only when the server or link is broken. But in Dual-Stack scenarios, the problem becomes more frequent and serious.

In Dual-Stack LAN/WLAN network or intranet, the core router or AC often plays the role of DHCP server, and the clients are serval thousands PC or mobile phones. If the server is configured in IPv6-only, the dual-stack or IPv4-only clients will broadcast DHCPDISCOVER messages endlessly in the LAN or WLAN. The thousands clients will cause a DDOS-like attack to all the servers in the network.

This situation may occur when the networks or serveices gradually updated to IPv6-Only.

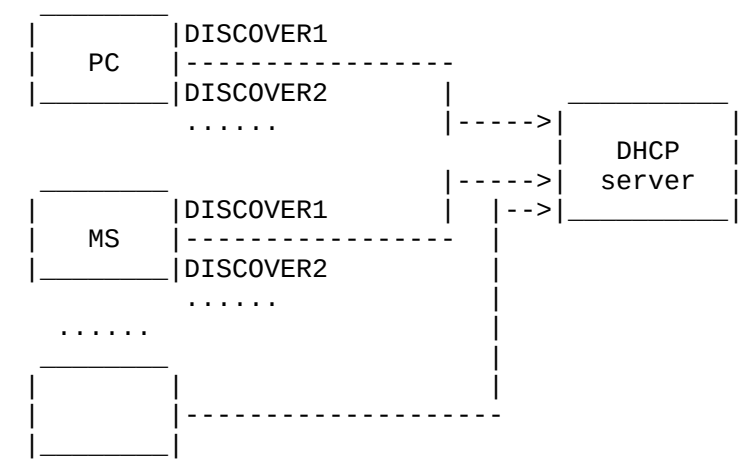


Figure 1: DHCPDISCOVER flood in LAN/WLAN

To avoid this problem, most of the terminals creat backoff algorithms which can help them retransmit DHCPDISCOVER message in different frequency according to their state machine in different Operating Systems, because there is no specific defenition in RFCs to restrict the terminals behaviors when the server is down or in a dual-stack scenario as discripted upwards. But the same point of almost all the verious Operating Systems is that they could not stop DHCPDISCOVER requests enven to an IPv6-only server. We test some of the most popular terminals' OS in WLAN, the results are illuminated as below.

DHCP Discovery Packages Time Table

No	Windows7 Time	Windows7 Time offset	Windows XP Time	Windows XP Time offset	IOS_5.0.1 Time	IOS_5.0.1 Time offset	Android_2.3.7 Time	Android_2.3.7 Time offset	Symbian_S60 Time	Symbian_S60 Time offse
1	0		0		0.1		7.8		0	
2	3.9	3.9	0.1	0.1	1.4	1.3	10.3	2.5	2	2
3	13.3	9.4	4.1	4	3.8	2.4	17.9	7.6	6	4
4	30.5	17.2	12.1	8	7.9	4.1	33.9	16	8	2
5	62.8	32.3	29.1	17	16.3	8.4	36.5	2.6	12	4
6	65.9	3.1	64.9	35.8	24.9	8.6	reconnect		14	2
7	74.9	9	68.9	4	33.4	8.5	56.6	20.1	18	4
8	92.1	17.2	77.9	9	42.2	8.8	60.2	3.6	20	2
9	395.2	303.1	93.9	16	50.8	8.6	68.4	8.2	24	4
10	399.1	3.9	433.9	340	59.1	8.3	84.8	16.4	26	2
11	407.1	8	438.9	5	127.3	68.2	86.7	1.9	30.1	4.1
12	423.4	16.3	447.9	9	128.9	1.6	reconnect		32.1	2
13	455.4	32	464.9	17	131.1	2.2	106.7	20	36.1	4
14	460.4	5	794.9	330	135.1	4	111.4	4.7	38.1	2
15	467.4	7	799.9	5	143.4	8.3	120.6	9.2	42.1	4
16	483.4	16	808.9	9	151.7	8.3	134.9	14.3	44.1	2
17	842.9	359.5	824.9	16	160.4	8.7	136.8	1.9	48.2	4.1
18	846.9	4	1141.9	317	168.8	8.4	reconnect		50.2	2

Figure2:Terminals DHCPDISCOVER requests when Server’s DHCP module
is down

In figure 2:

For Windows7, it seems to initiate 8 times DHCPDISCOVER requests in about 300s interval.

For WindowsXP, firstly it launches 9 times DHCPDISCOVER messages, but after that it cannot get any response from the server, then it initiates 5 times requests in one cycle in around 330s intervals, and never stop.

For IOS5.0.1, it seems like WindowsXP. There are 10 times attempts in one cycle, and the interval is about 68s.

Symbian_S60 uses the simplest backoff method, it launches DISCOVER in every 2 or 4 seconds.

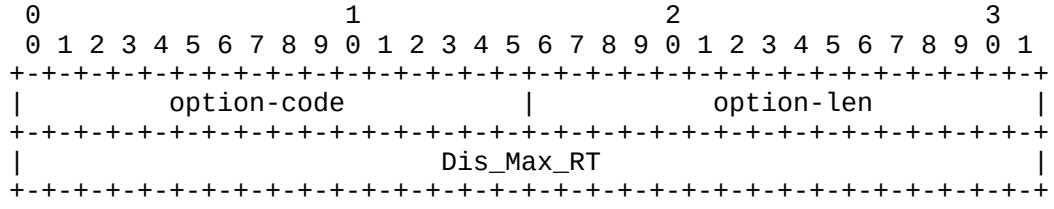
Android2.3.7 is the only Operating System which can stop DISCOVER

request by disconnect its wireless connection. It reboot wireless and dhcp connection every 20 seconds.

Obviously, DHCP server needs to weaken the traffic which is like DDoS attack caused by the clients when many DHCPv4 clients send discovery messages incessantly when the DHCPv4 server is configured no respond to Discover messages.

4. DHCPv6 solution

According to the definition of DHCPv6 option in RFC3315 [RFC3315], a new option named OPTION_Dis_Max_RT is defined to affect the retransmission of DHCPv4 DISCOVER message of the host. The format of OPTION_Dis_Max_RT is:



option-code	OPTION_Sol/Dis_Max_RT (TBD).
option-len	4.
Dis_Max_RT	DHCPv4 Discover retransmission time in seconds.

OPTION_Dis_Max_RT

The OPTION_Dis_Max_RT option needs IANA to assign a new Code to indicate. Its length (Len value) is 4 octets. Dis_Max_RT is the value of DHCPv4 Discover message retransmission time in the unit of second.

If Dis_Max_RT=0, server will respond Offer or other DHCP messages in normal;

If Dis_Max_RT>0, server won’t respond to Discover immediately, cliet should wait for resending Discover message later;

If Dis_Max_RT=FFFF, cliet should not send Discover message any more.

A DHCPv6 client MUST include the OPTION_Dis_Max_RT code in Option Request Option [RFC3115, section 22.7]. The DHCPv6 server MAY

include the OPTION_Dis_Max_RT in any response it sends to a client.

The process of this option is described below:

1. Client must initial the request code in the Option Request Option in the Discover messages.

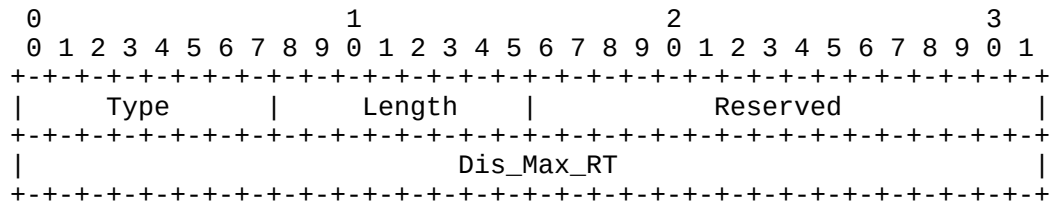
2. When server receives a request, it MUST assign an appropriate value in the response to the client. It can set FFFF in the Dis_Max_RT field when the dhcp module is turned off or according to the administrator's configuration.

5. RA solution

Neighbor Discovery for IPv6 defined in RFC4861[RFC4861] is a basic protocol of IPv6. It is used more widely than DHCPv6. When the value of M in Router Advertisment(RA) message is set, DHCPv6 can only be set to active. If M and O are not set, RA will be used to deliver the IPv6 prefix instead of DHCPv6. A new option is defined in Router Advertisment(RA) messages to be used to avoid frequent retransmission.

According to the definition of RA option in RFC4861 [RFC4861], a new option named Option_Dis_Max_RT is defined to affect the retransmission of DHCPv4 DISCOVER message.

The format of OPTION_Dis_Max_RT is:



Type	OPTION_Sol/Dis_Max_RT (TBD).
Length	8.
Reserved	Reserved.
Dis_Max_RT	DHCPv4 Discover retransmission time in seconds.

OPTION_Dis_Max_RT

The OPTION_Dis_Max_RT option needs IANA to assign a new Code to

indicate and its length (Len value) is 8 octets. Dis_Max_RT is the value of DHCPv4 Discover message retransmission time in the unit of second.

If Dis_Max_RT=0, server will respond Offer or other DHCP messages in normal;

If Dis_Max_RT>0, server won't respond to Discover immediately, cliet should wait for resending Discover message later;

If Dis_Max_RT=FFFF, cliet should not send Discover message any more.

The process is a little simpler than DHCPv6:

1. Server send RA with this option to cliet to tell it the intervals to resend Discover messages.

6. Security Considerations

The security problem is under disscussion.

7. IANA Considerations

IANA is requested to assign an option code from the "DHCP Option Codes" Registry for OPTION_DIS_MAX_RT.

8. Refrences

(1) RFC[2131] Dynamic Host Configuration Protocol

(2) RFC[3315] Dynamic Host Configuration Protocol for IPv6(DHCPv6)

(3) RFC[4861] Neighbor Discovery for IP version 6

Authors' Addresses

Tianle Yang
China Mobile
32, Xuanwumenxi Ave.
Xicheng District, Beijing 100053
China

Email: yangtianle@chinamobile.com

Li Lianyuan
China Mobile
32, Xuanwumenxi Ave.
Xicheng District, Beijing 100053
China

Email: lilianyuan@chinamobile.com

Qiongfang Ma
China Mobile
32, Xuanwumenxi Ave.
Xicheng District, Beijing 100053
China

Email: maqiongfang@chinamobile.com